Chapter 1: Commutators and 3-Cycles

Our aim in these notes is to use Rubik's magic cube to give insight into concepts from group theory. We do not assume any knowledge of group theory. We hope that what we have to say will be of interest to readers either with or without a group theory background, and to readers who are novices or experienced cubists alike.

In this chapter we introduce two classes of useful operations, the corner and edge 3-cycles. These are sufficient to solve the cube, though in this chapter we will not give an algorithm for solving the cube. Rather we will examine one example each of these two classes, with a particular question in mind. Each of these two particular operations is surprising because it only affects 3 pieces, in one case 3 corners, and in the other case 3 edges. Such a process is useful because, as one solves the cube one arrives at positions where most but not all of the pieces are in the right position. To finish the puzzle, one needs moves that only affect a few pieces, so that one may manipulate the few that are misplaced without disturbing the ones which are already correctly positioned.

But *why* is it that these particular operations work? Why does each of them move 3 pieces and none others? It is a minor miracle that this can be accomplished with eight or ten turns of the cube. We will give an explanation for this phenomenon by showing that the two moves in question are *commutators*.

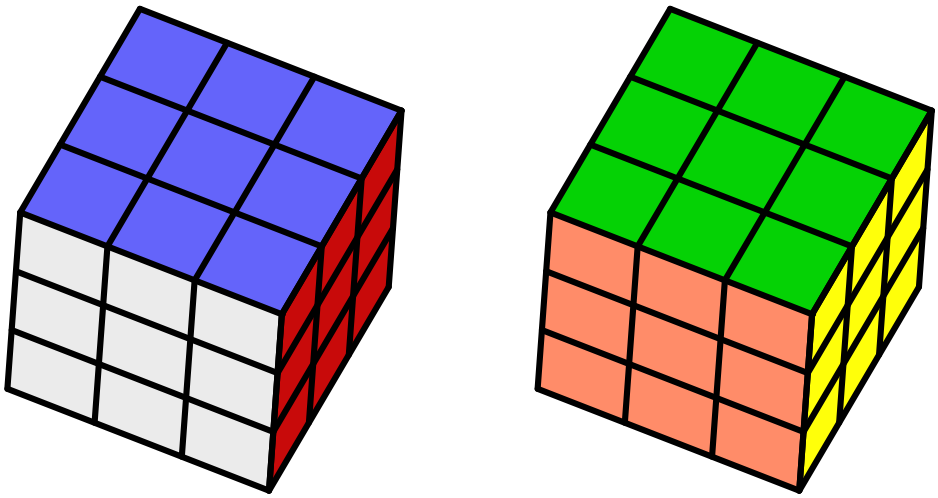

Figure 1. Top and Bottom views of the solved cube.

One thing Rubik has always insisted on from the manufacturers is a coloring scheme is followed to this day. Red is opposite orange, blue opposite green and yellow opposite white. Your cube should look like Figure 1, though it might be a mirror image.

Figure 1 shows the whole cube in two views. The cube is viewed from the top in the left figure, and from the bottom in the right figure.

It is also useful to give a single "sterographic" image of the cube showing *most* of the cube in a single view (Figure 2). Everything except the bottom (green) face is visible.

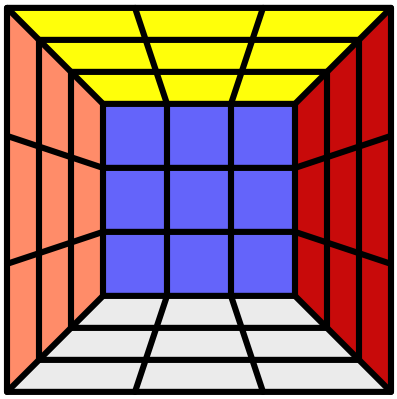

Figure 2. Stereographic map of the solved cube.

Following cube pioneer David Singmaster we label the six sides of the cube "up," "down," "left," "right," "front," "back," and "down," with the corresponding abbrievi-ations U (blue in Figure 1), D (green), L (orange), R (red), F (white) and B (yellow). The terms "up" and "down" are used instead of "top" and "bottom" since the letter B is already taken.

Singmaster's notion extends to operations on the cube. If X is one of the faces of the cube, then X denotes the operation of rotating the X face through an angle of $\frac{\pi}{2} = 90°$ in the *clockwise* direction, while X^{-1} denotes the operation of rotating the X face through an angle of $\pi/2$ in the counterclockwise direction. Thus, starting with the solved cube in Figure 1, after R^{-1} the cube looks as in Figure 3. If g is any operation of the cube we'll denote by g^n the operation g done n times, and 1 will denote the operation which doesn't change anything, so if X is the rotation of a face, $X^4 = 1$ and $X^3 = X^{-1}$.

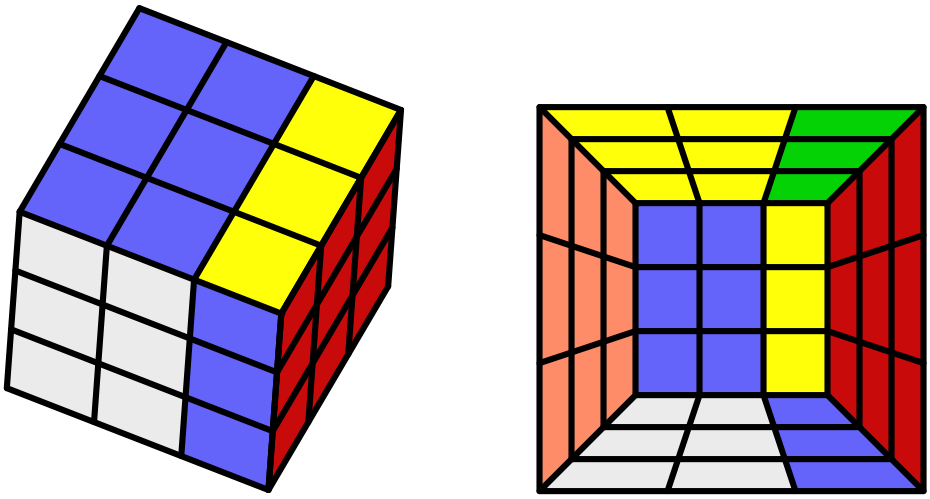

Figure 3. After R^{-1} is applied to a solved cube.

We can concatenate operations of the cube. Thus if g and h are operations of the cube, then gh is the operation consisting of first doing g, then doing h. We think of this as a sort of multiplication, making the set of operations of the cube into a mathematical object, known as a *group*. Note the order in which we do the operations: we proceed from left to right.

If g is an operation of the cube, then g^{-1} denotes the operation which undoes whatever g does. This is standard mathematical notation. The alternative notation g^{-1} was introduced by Singmaster for brevity. It is often used in discussing the cube, but in other applications of group theory, it is not a standard notation. We will also denote by 1 the group element which does nothing. The inverse g^{-1} is therefore characterized by the rule

$$gg^{-1} = g^{-1}g = 1 \tag{1}$$

The following fact is basic:

$$(gh)^{-1} = h^{-1}g^{-1} \tag{2}$$

To see that this is true, multiply gh by $h^{-1}g^{-1}$. We get $ghh^{-1}g^{-1} = gg^{-1} = 1$. This means that $h^{-1}g^{-1}$ undoes what gh does, and so it is the inverse of gh.

If g and h are given then ghg^{-1} is called the *conjugate* of h by g. *Conjugation*, the process which takes h into ghg^{-1} is a magical operation which we'll see a lot of. We note a couple of its important properties. We have:

$$(ghg^{-1})^{-1} = gh^{-1}h^{-1} \tag{3}$$

because using (2), $(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1}$ and $(g^{-1})^{-1} = g$. Also

$$g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) \tag{4}$$

because on the right side, the $g^{-1}g$ cancel.

Try the operation $FRF^{-1}LFR^{-1}F^{-1}L^{-1}$. Starting from the solved cube in Figure 1, the configuration in Figure 4 results.

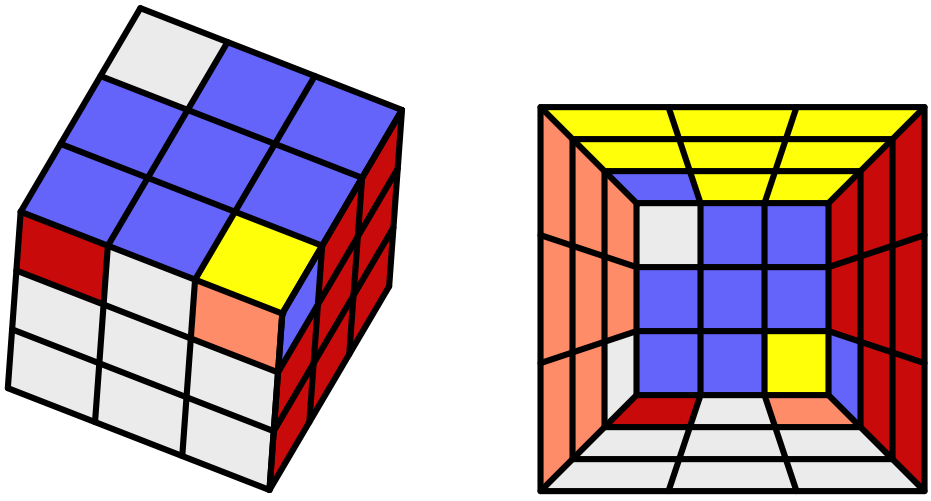

Figure 4. The corner 3-cycle $FRF^{-1}LFR^{-1}F^{-1}L^{-1}$.

Notice that *only three pieces are out of place*, namely the three corner pieces in the upper back left, upper front right and the upper front left positions. These are permuted cyclicly. This operation is therefore called a *corner 3-cycle*.

Let us try to understand why $FRF^{-1}LFR^{-1}F^{-1}L^{-1}$ has such a simple effect. Why does it only affect three pieces? After all, if you apply eight random rotations, they will probably leave the cube looking very scrambled. What's so special about this particular sequence? It turns out this question has a nice answer.

If g and h are two operations of the cube, denote $[g,h] = ghg^{-1}h^{-1}$. This is called the *commutator* of g and h. The reason for this term is that

$$[g,h] = 1 \text{ if and only if } gh = hg. \tag{5}$$

To prove this, assume $[g,h] = 1$. Multiplying this equation on the right by hg we get $ghg^{-1}h^{-1}hg = hg$, and $ghg^{-1}h^{-1}hg = ghg^{-1}g = gh$ so $gh = hg$. You can check that this reasoning is reversible.

We say g and h *commute* if $gh = hg$. So (5) says that the commutator of g and h is trivial if and only if g and h commute with each other.

If g is an operation on the cube, let the *support* of g, denoted $\text{supp}(g)$, be the set of pieces which are changed by g. We note that if two operations g and h have disjoint support—that is, if $\text{supp}(g) \cap \text{supp}(h)$ is the empty set—then g and h commute. (This is obvious!) For example L and R have disjoint supports, namely, the support of L consists of the pieces on the left side of the cube, and the support of R consists of the pieces on the right, and there is no overlap between these two sets. Therefore $LR = RL$ and so $[L,R] = 1$.

Now if g and h are two operations whose supports have only a *small* amount of overlap, then g and h will *almost* commute. This means that $[g,h]$ will be an operation which affects only a few pieces. Yet it will not be the identity. Consider $g = FRF^{-1}$, $h = L$. The effect of g is shown in Figure 5.

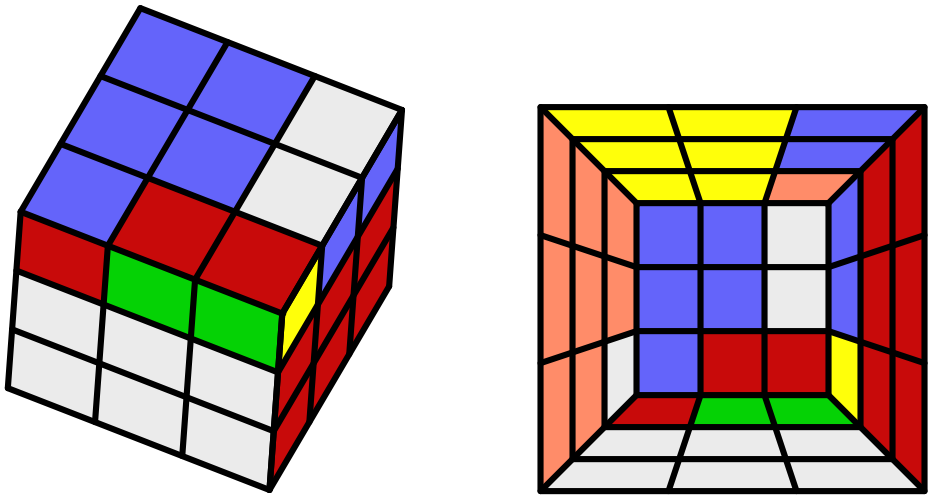

Figure 5. The effect of FRF^{-1}.

Of course $h = L$ only affects the nine pieces on the left, and of these, Figure 5 shows that $g = FRF^{-1}$ only affects a single piece, the upper front left corner. Since there is little overlap between the supports of g and h these operations *almost* commute, and so their commutator is *almost* trivial, that is, $[g, h] = FRF^{-1}LFR^{-1}F^{-1}L^{-1}$ should only affect a small number of pieces. In fact, it only affects three, as the following result shows.

Proposition 1. *Suppose that* $\mathrm{supp}(g) \cap \mathrm{supp}(h)$ *consists of a single piece. Then* $[g, h]$ *is a* 3*-cycle.*

We won't give a formal proof of this until the next chapter. For the time being the heuristic arguments we've given will suffice.

Let X_{m} denote the *middle layer move* that rotates just the middle layer *between* the X and Y faces clockwise (looking at X face) in an angle of $\frac{\pi}{2} = 90°$. (See Figure 6.)

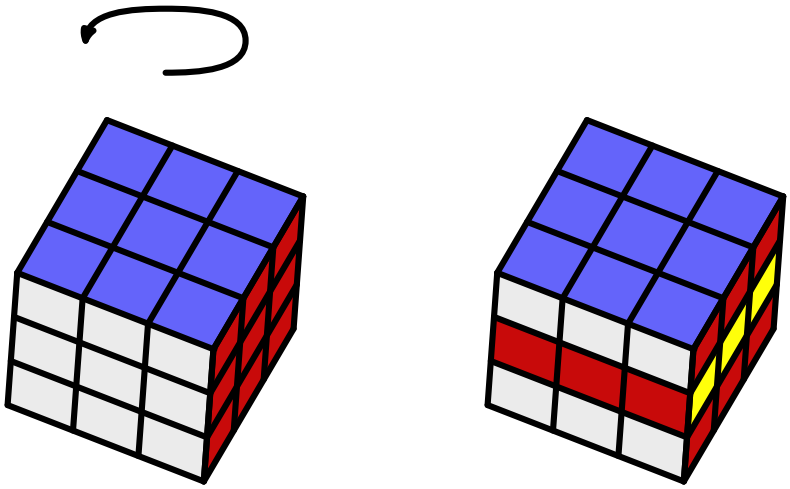

Figure 6. Left: initial state. Right: after the middle layer move U_{m}

In addition to the corner 3-cycles, *edge* 3*-cycles* are also in the cubist's repertoire. For example, consider $LF^{-1}L^{-1}F_{\mathrm{m}}^{-1}LFL^{-1}F_{\mathrm{m}}$. Figure 7 shows the result of this edge 3-cycle.

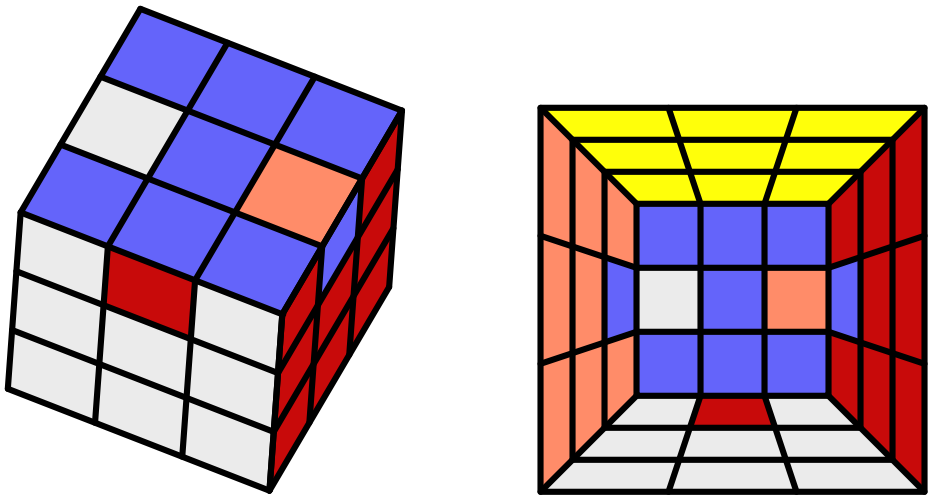

Figure 7. The edge 3-cycle $LF^{-1}L^{-1}F_{\mathrm{m}}^{-1}LFL^{-1}F_{\mathrm{m}}$.

This is the commutator $[LF^{-1}L^{-1}, F_{\mathrm{m}}^{-1}]$. Here $LF^{-1}L^{-1}$ has the effect shown in Figure 8.

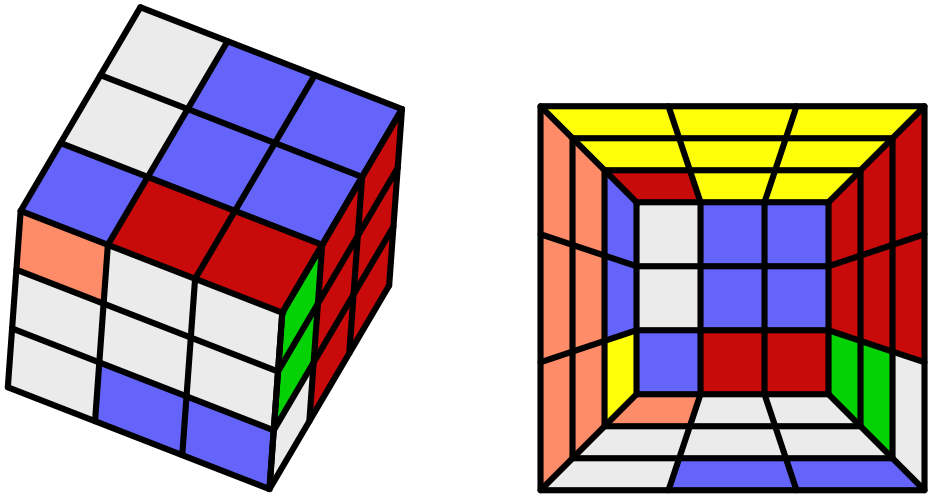

Figure 8. The effect of $LF^{-1}L^{-1}$.

The support of F_{m}^{-1} consists of the middle slice between the front and back rows, and of these, only the piece in the upper left edge is affected by $LF^{-1}L^{-1}$, so Proposition 1 again implies that only three elements are affected by $[LF^{-1}L^{-1}, F_{\mathrm{m}}^{-1}]$.

Not every edge 3-cycle can be so easily neatly as this one. Try

$$RBLFUF^{-1}L^{-1}B^{-1}R^{-1}U^{-1}$$

(Figure 9).

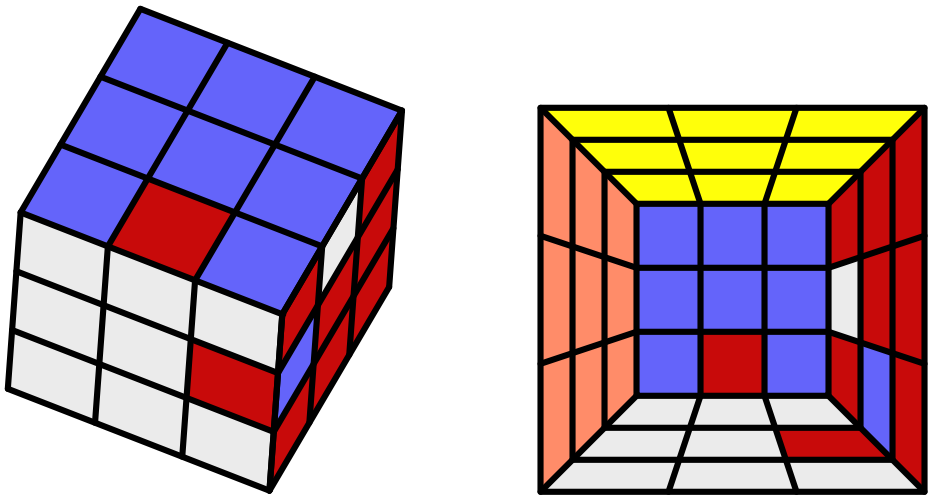

Figure 9. The effect of $RBLFUF^{-1}L^{-1}B^{-1}R^{-1}U^{-1}$

This pleasant and easily remembered operation is a commutator, $[RBLF, T]$. The fact that it is an edge 3-cycle does not follow simply from Proposition 1. Still the ideas of this section are definitely relevant to understanding how this operation works. (Think carefully about the effect of $RBLF$ on the top face.)

We note that when the cube is manipulated using only the motions U, D, L, R, F and B, the center pieces rotate but do not otherwise move. If you apply one of these motions the center pieces turn but don't go anywhere. So even after applying these many times, although the cube looks very scrambled the centers are in their standard locations (Figure 10).

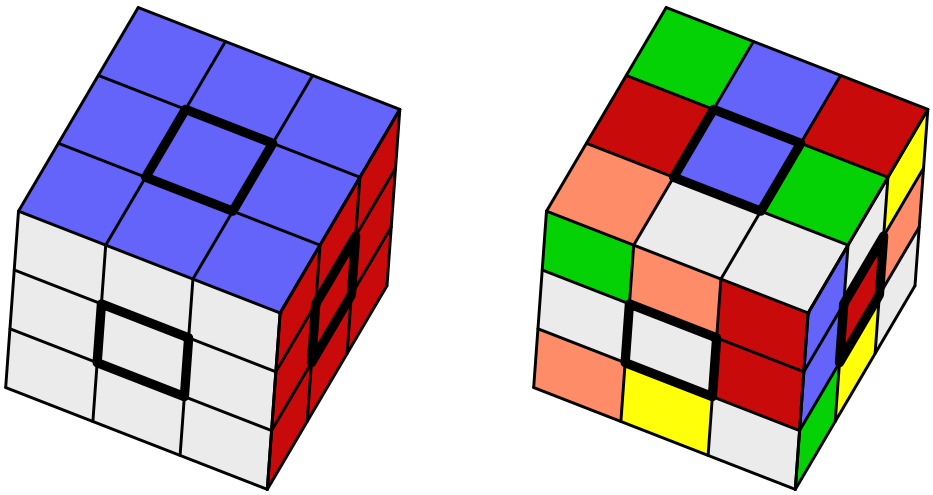

Figure 10. When the cube is scrambled, the center pieces do not move!

This fact, that the center pieces never move, is the key to the *mechanism* of the cube, and you will see what I mean if you take one apart. (To disassemble the cube, rotate one face by $\frac{\pi}{4} = 45°$, then pry out one of the four middle pieces. The cube will then

come apart. It can be reassembled by reversing the process.) Of course you don't actually need to know *anything* about the actual mechanism to see that the center pieces never move—this is a consequence of the fact that the rotation of any face doesn't move any center piece, except to turn it.

Because of this property we may consider two different realizations of the group of the cube. In the smaller realization, which we denote as $\mathfrak{G}$, we always insist that the center pieces have the same spatial orientation. The elements of the group consist of the motions of the cube generated by U, D, L, R, F and B.

The *extended* group $\mathfrak{E}$ of the cube consists of all motions of the cube, including rotations which move the center pieces. In addition to $\mathfrak{G}$, contains the group R of *rotations* of the entire cube. Elements of R do not affect the pattern of the cube, only its orientation. The reason these motions don't essentially affect anything is that everything in the cube moves together. For example, if X is a face, let $X_{\mathrm{c}} \in R$ denote the rotation of the *entire cube* by an angle of $\frac{\pi}{2} = 90°$ clockwise around the X face (Figure 11).

Returning to the extended group $\mathfrak{E}$, if g is in $\mathfrak{E}$, then there is a rotation $r \in R$ which restores the locations of the locations of the faces to their original positions. Then $gr \in \mathfrak{G}$. For example if $g = X_{\mathrm{m}}$, we should take $r = X_{\mathrm{c}}^{-1}$.

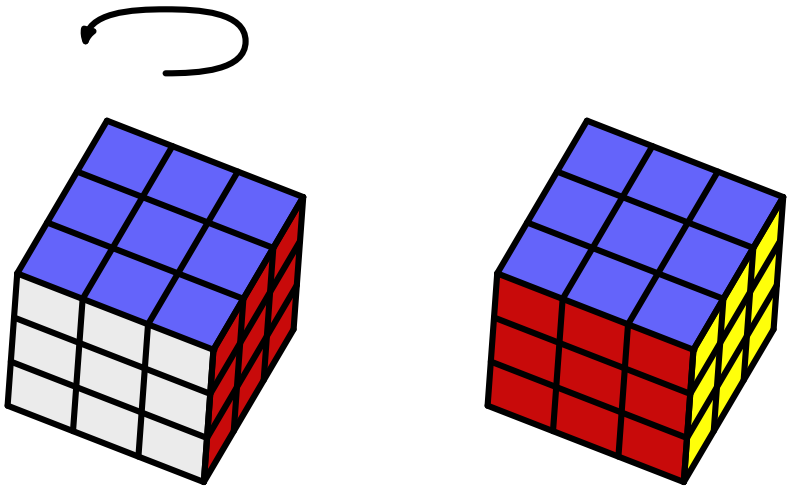

Figure 11. Left: initial state. Right: after the rotation U_{c}

We see that if $g \in \mathfrak{E}$, we may apply an element r of R, which, being a rotation of the whole cube does not essentially affect the condition of the cube, and transform g into an element rg of $\mathfrak{G}$. As an example, if $g = F_{\mathrm{m}}$ we can take $r = F_{\mathrm{c}}^{-1}$ and we find (Figure 12) that

$$F_{\mathrm{m}} F_{\mathrm{c}}^{-1} = F^{-1} B, \qquad F_{\mathrm{m}} = F^{-1} B F_{\mathrm{c}} = F_{\mathrm{c}} F^{-1} B, \tag{6}$$

so $gr = F^{-1}B \in \mathfrak{G}$. Because of this fact, there is nothing we can do in the extended group $\mathfrak{E}$ that we cannot do in $\mathfrak{G}$ itself.

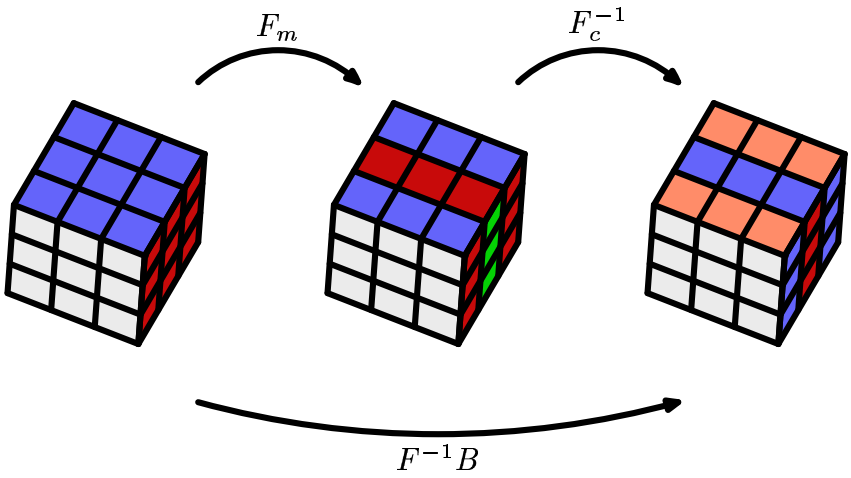

Figure 12. Showing that $F_{\mathrm{m}}F_{\mathrm{c}}^{-1} = F^{-1}B$

For this reason it might seem that there is no real advantage to considering the extended group. Nevertheless sometimes it is better to work in the extended group, and as evidence of this claim, we will now return to the edge 3-cycle $LF^{-1}L^{-1}F_{\mathrm{m}}^{-1}LFL^{-1}F_{\mathrm{m}}$ in Figure 7. First we consider how to write this without making use of the extended group element F_{m}.

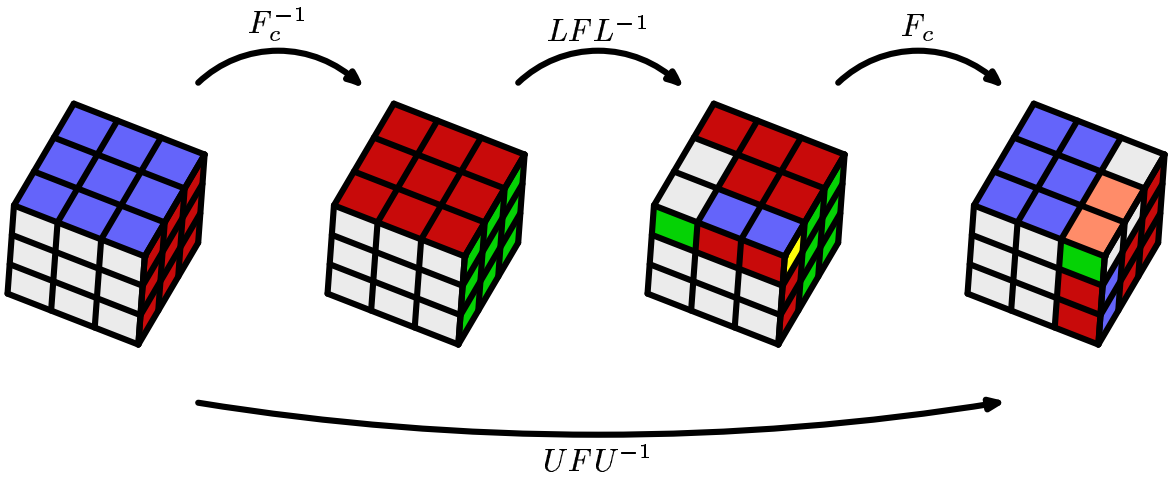

Figure 13. Applying F_{c}^{-1}, then LFL^{-1} and F_{c} gives the same result as UFU^{-1}.

Using (6) we have

$$LF^{-1}L^{-1}F_{\mathrm{m}}^{-1}LFL^{-1}F_{\mathrm{m}} = LF^{-1}L^{-1}FB^{-1}F_{\mathrm{c}}^{-1}LFL^{-1}F_cF^{-1}B.$$

Now (Figure 13)

$$F_{\mathrm{c}}^{-1}(LFL^{-1})F_{\mathrm{c}} = UFU^{-1}. \tag{7}$$

Using this, our edge 3-cycle becomes

$$LF^{-1}L^{-1}FB^{-1}UFU^{-1}BF^{-1} \tag{8}$$

The last expression involves only operations in the group $\mathfrak{G}$.

Although (8) rewrites the edge three cycle in a form only involving elements of the group $\mathfrak{G}$, avoiding the element F_{m} of the extended group, we prefer the original expression (Figure 7) because it exhibits the element as a commutator, and Theorem 1 is not applicable.

Moreover, (Figure 7) is a more *ergonomic* form of the operation. By this we mean that from the point of view of someone who is trying to solve the cube in practice, (Figure 7) is easier both to remember and to perform in practice.

Finally, our mathematical universe will be richer if we work in the extended group $\mathfrak{E}$. Later we will see that the group $\mathfrak{E}$ is a *semidirect product* of the subgroups $\mathfrak{G}$ and R, and this will give us our first example of this important construction.

Exercise. *Invent a few more corner and edge 3-cycles. Make a table of the processes you discover.*

Chapter 2: The Symmetric Group

In Chapter 1 we made use of group theory concepts without actually defining the term *group*. A *group* is a set G with a multiplication law sending any pair of elements to their product $x \cdot y = xy$. The group law must be associative:

$$(xy)z = x(yz)$$

and there must be a distinguished *unit* element $1 \in G$ such that

$$1 \cdot x = x \cdot 1 = x.$$

Finally, for every $x \in G$ there must be an *inverse element* x^{-1} such that

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

If the group G satisfies the commutative law $ab = ba$, it is called commutative or *abelian*. For abelian groups, we sometimes use additive notation, writing $+$ for the group law and 0 for the identity element. Thus for example $\mathbb{Z}$ is a group with addition as the group law.

If N is the number of elements in a group, we call N the *order* of the group. (It may be infinite.)

If G and H are groups, a *group homomorphism* is a map $\phi : G \to H$ such that $\phi(x_1x_2) = \phi(x_1)\phi(x_2)$, x_1, $x_2 \in G$.

A *subgroup* of a group G is a subset $K \subset G$ containing 1 which is closed under multiplication and inverses. It inherits a group structure from G. If G is a group it has two obvious subgroups, namely G itself and $\{1\}$. (We will sometimes denote the latter subgroup as just 1.)

If $\phi : G \to H$ is a homomorphism, let $K = \{g \in G | \phi(g) = 1\}$. It is automatically a subgroup, as you may easily check. It is called the *kernel* of ϕ, denoted $\ker(\phi)$.

Proposition 2. *Let $\phi : G \to H$ be a homomorphism. Then ϕ is injective if and only if the kernel K of ϕ is trivial, that is, if $K = 1$.*

Proof. If $x \in K$ and $x \neq 1$ then $\phi(x) = \phi(1)$ so ϕ is not injective. On the other hand suppose that $K = \{1\}$ and $\phi(x) = \phi(y)$. Then $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = 1$ so $xy^{-1} \in K$, so $xy^{-1} = 1$, so $x = y$. Therefore ϕ is injective. ∎

Homomorphisms are abundant. Recognizing and using them is important. Let us give an example. If $g \in G$ is a fixed element of a group G, define $\phi : G \to G$ by $\phi(x) = gxg^{-1}$. Then (4) implies that ϕ is a homomorphism.

As another example, let $\mathfrak{G}$ be the group of the Rubik's cube as in Chapter 1, and let $\mathfrak{G}_2$ be the group of the smaller 2×2 cube. The operations U, D, R, L, F and B all make

sense for the 2×2 cube. We may map $\mathfrak{G} \to \mathfrak{G}_2$ by copying each motion of the 3×3 cube with the corresponding motion of the 2×2 cube. This map is a homomorphism.

If X and Y are sets, then a map $f : X \to Y$ is called *injective* if for all $x_1, x_2 \in X$, if $f(x_1) = f(x_2)$ then $x_1 = x_2$ $(x_1, x_2 \in X)$. It is called *surjective* if every element in y is $f(x)$ for some $x \in X$. If f is both injective and surjective, it is called *bijective*. Then for each $y \in Y$ there is a unique $x \in X$ such that $f(x) = y$ and we denote $f^{-1}(y) = x$. This is the *inverse map* $f^{-1} : Y \to X$.

If $f : X \to Y$ and $g : Y \to Z$ are maps, then $g \circ f : X \to Z$ denotes the *composition map*, $(g \circ f)(x) = g\big(f(x)\big)$. The composition is also denoted as simply gf. If f and g are bijections then so is $g \circ f$ and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

The *identity map* $I_X : X \to X$ is the map $1_X(x) = x$. If $f : X \to Y$ is a bijection then the defining property of $f^{-1} : Y \to X$ may be expressed by the identities $f^{-1} \circ f = 1_X$, $f \circ f^{-1} = 1_Y$.

An important group for us is the *symmetric group* S_n. Let $N = \{1, 2, \cdots, n\}$. (Actually N can be any set with n elements.) The set S_n consists of all bijective mappings $N \to N$. Elements of S_n are called *permutations*. The group law is composition of mappings. Thus if $\sigma, \tau \in S_n$ let $\sigma\tau : N \to N$ is the composition $\sigma \circ \tau$. Since $(\sigma\tau)(n) = \sigma\big(\tau(n)\big)$, τ is applied first, so multiplication of permutations, unlike the multiplication in the group $\mathfrak{G}$ of the Rubik's cube, proceeds from right to left.

Proposition 3. *S_n is a group with $n!$ elements.*

Proof. We may count these bijections as follows. There are n choices for $\sigma(1)$. Once $\sigma(1)$ is chosen, since σ is supposed to be bijective, $\sigma(2)$ cannot be $\sigma(1)$, so there are only $n - 1$ choices for $\sigma(2)$. Then there are $n - 2$ choices for $\sigma(3)$, and so on. ■

We introduce two notations for elements of the symmetric group. Let us consider $\sigma \in S_6$ defined by

$$\sigma(1) = 4; \qquad \sigma(2) = 5; \qquad \sigma(3) = 6;$$
$$\sigma(4) = 3; \qquad \sigma(5) = 2; \qquad \sigma(6) = 1.$$

One notation writes this by placing $\sigma(i)$ below i, as follows:

$$\sigma = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 4\ 5\ 6\ 3\ 2\ 1 \end{pmatrix}. \tag{9}$$

The other notation, called *cycle notation*, writes this as

$$\sigma = (1436)(25). \tag{10}$$

Here $(s_1\, s_2\, \cdots s_k)$ denotes the permutation which sends $s_i \to s_{i+1}$ and $s_k \to s_1$. Such a permutation is called a *k-cycle*. A 2-cycle is also called a *transposition*. We could also write (10) as $(52)(3614)$.

Notice that the two cycles in the second representation (10), namely (1436) and (25) affect disjoint sets of letters. We call the *support* $\mathrm{supp}(\sigma)$ the set of letters which are moved. The support of (1437) is $\{1, 3, 4, 7\}$, and the support of (25) is $\{2, 5\}$. These sets are disjoint, so we say the cycles (1436) and (25) are *disjoint*. Clearly this implies that they commute.

Proposition 4. *Any permutation can be written as a product of disjoint cycles.*

Proof. This proposition is really obvious if one understands what it means. See what was done with the permutation (9) above. It is clear that this can be done for any permutation. ■

As an example, let us compute the product (1562)(2673). By "compute," we mean we wish to express this product as a product of disjoint cycles. (We will see that it is a single 5-cycle.) The cycles (1562) and (2673) are *not* disjoint because their supports have 2 and 6 in common. Remembering that we multiply from right to left, $2 \to 6 \to 2$ is unchanged by (1562)(2673), while $1 \to 1 \to 5$, , $5 \to 5 \to 6$, $6 \to 7 \to 7$, $7 \to 3 \to 3$ and $3 \to 2 \to 1$. Thus

$$(1562)(2673) = (15673)(2) = (15673). \tag{11}$$

(There is no need to include the 1-cycle (2) since it doesn't do anything; it is just another notation for the identity element.)

The cube has 26 pieces, of which 6 are the centers, and do not move. So actually there are 20 pieces which get permuted when the cube is worked, 8 corners and 12 edges. We label these $\{1, 2, 3, \cdots, 20\}$ in some way. After an operation M of the cube a permutation σ of the 20 pieces results. We define a map $\phi_{\text{cube}} : \mathfrak{G} \to S_{20}$ by

$$\phi_{\text{cube}}(M) = \sigma. \tag{12}$$

Similarly, using just the corners, we get a homomorphism $\phi_{\text{corner}} : \mathfrak{G} \to S_8$, or using just the edges we get a homomorphism $\phi_{\text{edge}} : \mathfrak{G} \to S_{12}$.

At first it may seem surprising that this works, since in $\mathfrak{G}$ multiplication proceeds from left to right while in S_n multiplication proceeds from right to left. Specifically, to show that ϕ_{cube} is a homomorphism, we need to show that

$$\phi_{\text{cube}}(M_1\, M_2) = \phi_{\text{cube}}(M_1)\, \phi_{\text{cube}}(M_2). \tag{13}$$

Now on the left side $M_1\, M_2$ means performing first M_1, then M_2, while on the right side, $\phi_{\text{cube}}(M_1)\, \phi_{\text{cube}}(M_2)$ means first performing $\phi_{\text{cube}}(M_2)$, then $\phi_{\text{cube}}(M_1)$. This reversal is at first vexing.

We will postpone the proof that (13) always works, but accept it for the time being. But let us carefully work out an example. We will work with ϕ_{corner} for simplicity, and show that $\phi_{\text{corner}}(RF) = \phi_{\text{corner}}(R)\phi_{\text{corner}}(F)$.

We begin by computing $\phi_{\text{corner}}(F)$. Label the corners as in Figure 14 (left diagram).

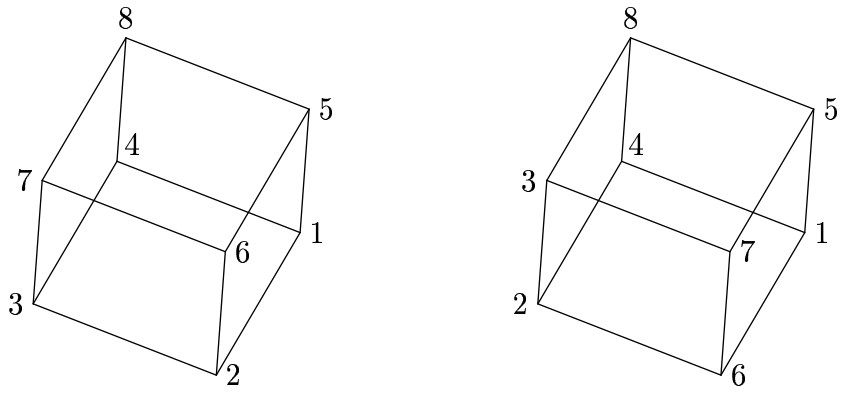

Figure 14. Left: initial configuration of the corners. Right: after F.

The left diagram gives a standard labelling of the corners. After rotating the front face (spanning 2, 3, 7 and 6) clockwise, the labelling on the right of Figure 14 results. The permutation $\phi_{\text{corner}}(F)$ of the corners consists of the 4-cycle (2673). For 2 gets replaced by 6, 6 by 7, 7 by 3 and 3 by 2, while 1, 4, 5 and 8 are untouched. Thus $\phi_{\text{corner}}(F) = (2673)$.

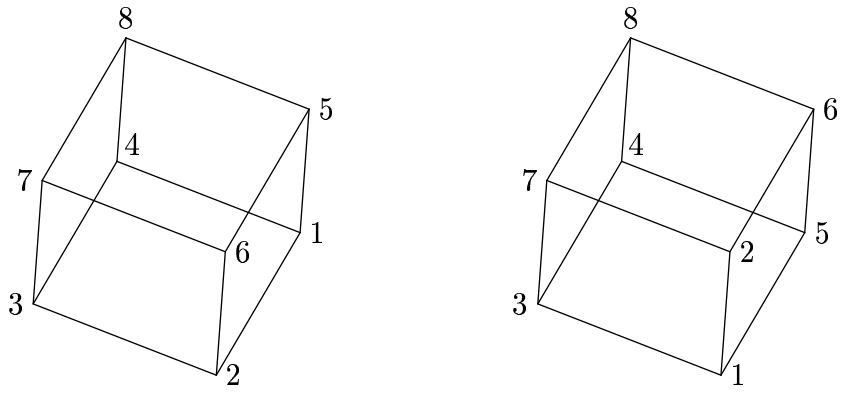

Figure 15. Left: initial configuration of the corners. Right: after R.

Similarly we compute $\phi_{\text{corner}}(R) = (1562)$. This computation is shown in Figure 15. The initial configuration is on the left, and after R we get the configuration on the right. 1 has been replaced by 5, 5 by 6, 6 by 2 and 2 by 1.

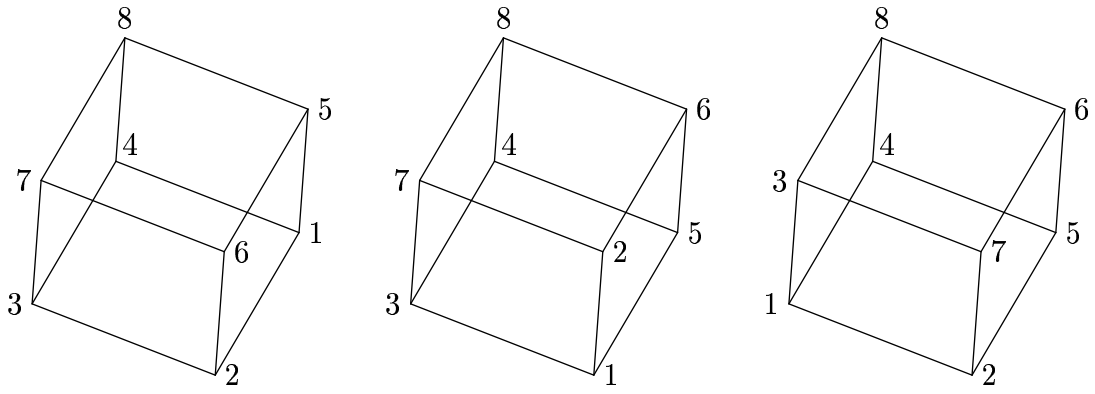

Figure 16. Left: Initial. Middle: After R. Right: After R then F.

Now let us confirm that

$$\phi_{\text{corner}}(RF) = \phi_{\text{corner}}(R)\,\phi_{\text{corner}}(F).$$

We've already found that $\phi_{\text{corner}}(F) = (2673)$ and $\phi_{\text{corner}}(R) = (1562)$. In Figure 16, we compute the effect of RF. The initial configuration is at left. After R, the middle diagram results. Then after F, the final diagram results. Comparing this result to the first diagram, we see that

$$\phi_{\text{corner}}(RF) = (15673).$$

On the other hand

$$\phi_{\text{corner}}(F)\phi_{\text{corner}}(R) = (1562)(2673).$$

Now $(1562)(2673) = (15673)$ by (11). This confirms (13) for this example.

The permutation $\phi_{\text{cube}}(M)$ does not capture exactly what a cube operation M does. This is because the pieces of the cube are not only changed in their *position* but also in their orientation. For example, try

$$RU^{-1}R^{-1}U_{\text{m}}^{-1}RUR^{-1}U_{\text{m}}R^2L^{-1}ULU_{\text{m}}^2L^{-1}U^{-1}LU_{\text{m}}^2R^2.$$

The position in Figure 17 results, in which all pieces are in their original positions, but two edge pieces are flipped.

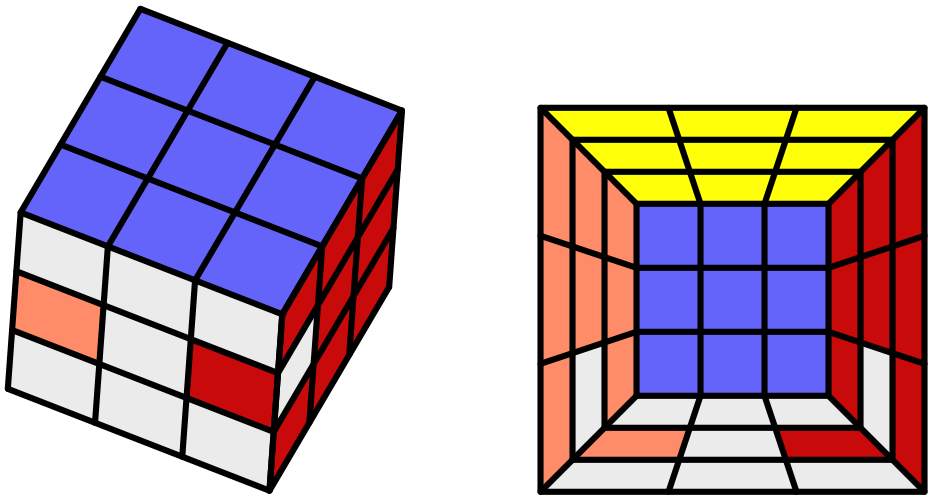

Figure 17. $RU^{-1}R^{-1}U_{\mathrm{m}}^{-1}RUR^{-1}U_{\mathrm{m}}R^2L^{-1}ULU_m^2L^{-1}U^{-1}LU_m^2R^2$.

It is interesting to note that there is no move which flips a *single* edge piece. In other words, the position in the left diagram in Figure 21 cannot be achieved.

A proof of this will be given in the next Chapter. But let us consider briefly how useful this fact is to someone who is trying to solve the cube. Suppose that one has solved the cube except for three edge pieces. An edge 3-cycle will then finish the puzzle.

But *which* precise operation? Suppose that g is an edge 3-cycle such that $\phi_{\mathrm{edge}}(g)$ is the right permutation. Then applying g will restore the edges to the correct locations, but will they have the right orientations? One choice of g will make this true. Luckily in selecting g we only have to worry about the orientations of two of the three edges, since if two are correctly positions, the third must be also. The reason for this is the fact, which we will prove in Chapter 3, that no operation in $\mathfrak{G}$ leaves all the pieces in position but flips a single edge (Figure 21, left).

Now try $RUR^{-1}URU^2R^{-1}L^{-1}U^{-1}LU^{-1}L^{-1}U^2L$. Two corner pieces twist (in opposite directions). See Figure 18. A variation is shown in Figure 19.

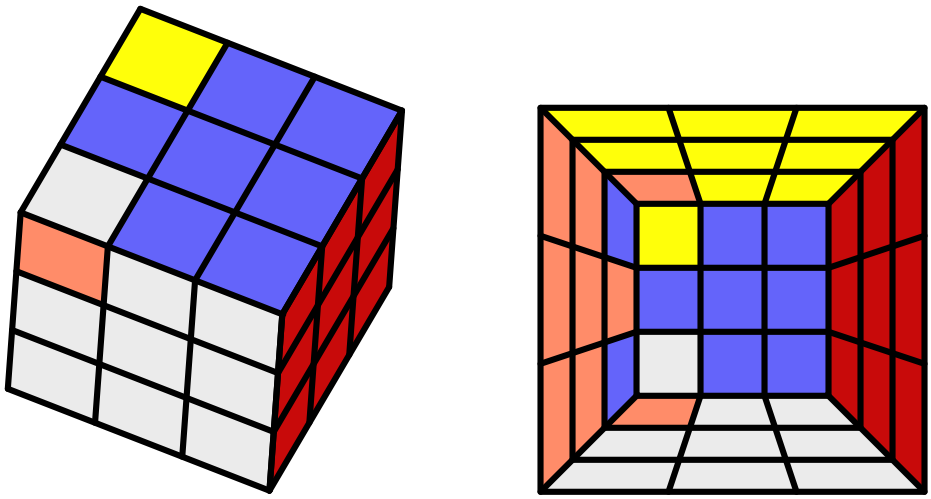

Figure 18. $RUR^{-1}URU^2R^{-1}L^{-1}U^{-1}LU^{-1}L^{-1}U^2L$.

These examples show are cube operations which do not move any pieces, only change their orientation. If M is such an operation, then $\phi_{\text{cube}}(M) = 1$.

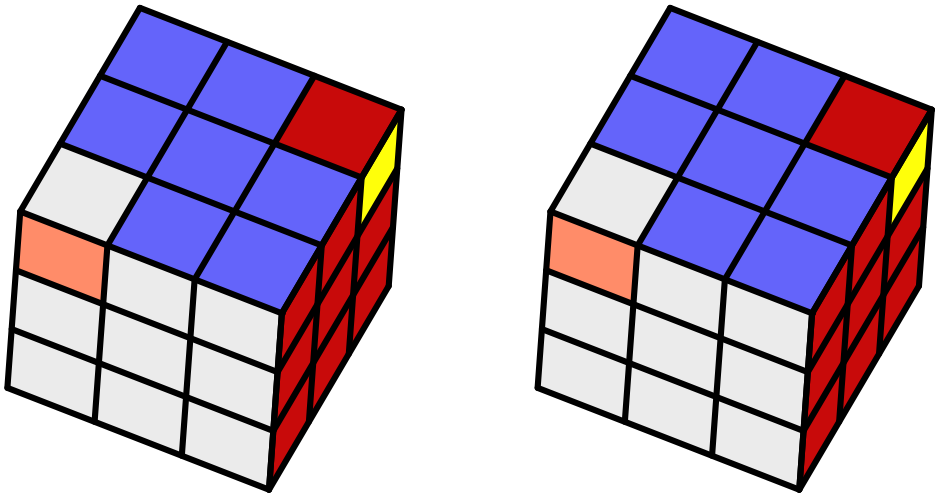

Figure 19. $BRUR^{-1}URU^2R^{-1}L^{-1}U^{-1}LU^{-1}L^{-1}U^2LB^{-1}$.

Chapter 3: The Alternating Group

The symmetric group S_n has an important subgroup known as the *alternating group* A_n. If $n > 1$, then A_n contains half the permutations in S_n, that is, $\frac{1}{2} \cdot n!$ of them. These permutations are called *even*, the others are called *odd*.

To prove that A_n exists, we construct a homomorphism $\epsilon : S_n \to \{\pm 1\}$. Let $x_1, \cdots, x_n$ be indeterminates. If $\sigma \in S_n$, and if $p(x_1, \cdots, x_n)$ is a polynomial, define

$$(\sigma p)(x_1, \cdots, x_n) = p(x_{\sigma(1)}, \cdots, x_{\sigma(2)}). \tag{14}$$

For example, if $\sigma = (12)$, applying σ to $x_1^2 + x_2 x_3$ gives $x_2^2 + x_1 x_3$.

Proposition 5. *If $\sigma, \tau \in S_n$ and $p(x_1, \cdots, x_n)$ is a polynomial, we have $\sigma(\tau p) = (\sigma\tau)p$.*

Proof. It is easy to make a mistake and "prove" incorrectly that $\sigma(\tau p) = (\tau\sigma)p$. We can avoid this by carefully introducing some auxiliary variables $y_i = x_{\sigma(i)}$. By (14),

$$\sigma(\tau p)(x_1, \cdots, x_n) = (\tau p)(x_{\sigma(1)}, \cdots, x_{\sigma_n}) = (\tau p)(y_1, \cdots, y_n) = \\ p(y_{\tau(1)}, \cdots, y_{\tau(n)}) = p(x_{\sigma\tau(1)}, \cdots, x_{\sigma\tau(n)}).$$

This completes the proof. ■

Apply σ to

$$\Delta(x_1, \cdots, x_n) = \prod_{i<j} (x_i - x_j).$$

We note that σ turns each $x_i - x_j$ into another $x_i - x_j$, or its negative. Therefore $\sigma\Delta = \pm\Delta$. We define $\epsilon(\sigma)$ to be this sign, that is, $\epsilon(\sigma)$ is defined by the equation

$$\sigma\Delta = \epsilon(\sigma)\Delta.$$

For example, if $n = 3$ then applying (12) to

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

gives

$$(x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -\Delta.$$

Thus $\epsilon\big((12)\big) = -1$. On the other hand, applying (123) to Δ gives

$$(x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = \Delta$$

since there are two sign changes. Therefore $\epsilon\big((123)\big) = 1$.

Proposition 6. *The map $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism.*

Proof. Applying $\tau \in S_n$ to Δ gives $\epsilon(\tau)\Delta$. Now applying σ gives $\epsilon(\sigma)\epsilon(\tau)\Delta$. On the other hand we could get the same result by applying $\sigma\tau$ in a single step, that is,

$$\epsilon(\sigma)\epsilon(\tau)\Delta = \epsilon(\sigma\tau)\,\Delta.$$

Therefore

$$\epsilon(\sigma)\epsilon(\tau) = \epsilon(\sigma\tau),$$

so $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism.

Now let $A_n = \{\sigma \in S_n | \epsilon(\sigma) = 1\}$.

Proposition 7. *A_n is a subgroup of S_n of order $\frac{1}{2}\,n!$.*

Proof. As the kernel of a homomorphism, A_n is a subgroup. We fix an element τ such that $\epsilon(\tau) = -1$. For example, we may take $\tau = (12)$. Then if $\sigma \in S_n$,

$$\epsilon(\tau\sigma) = \epsilon(\tau)\,\epsilon(\sigma) = -\epsilon(\sigma).$$

So $\sigma \in A_n$ if and only if $\epsilon(\sigma) = 1$, if and only if $\epsilon(\tau\sigma) = -1$, if and only if $\sigma\tau \notin A_n$. Thus the map

$$\sigma \mapsto \tau\sigma$$

is a bijection from A_n to its complement in S_n. It follows that A_n comprises exactly half the elements of S_n, that is, $\frac{1}{2}\,n!$. ■

Proposition 8. *If $1 \le p < q \le n$ then the 2-cycle (pq) is odd.*

Proof. Apply (pq) to Δ. We may identify the monomials $x_i - x_j$ which get their signs change. These are $x_p - x_i$ with $p < i < q$, $x_i - x_q$ with $p < i < q$, and $x_p - x_q$. There are $2(j-i)-1$ of these. Since this is odd, Δ gets multiplied by -1. Therefore $\epsilon\big((pq)\big) = -1$. ■

Proposition 9. *A k-cycle $(i_1 i_2 \cdots i_k)$ is odd if and only if k is even.*

Proof. We can factor

$$(i_1 i_2 \cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k).$$

Applying ϵ and using Proposition 8,

$$\epsilon\big((i_1 i_2 \cdots i_k)\big) = (-1)^{k-1}.$$

So this is an odd permutation if and only if k is even. ■

We may now identify the elements in A_n.

Theorem 10. *If $\sigma \in S_n$, then σ is even if and only if there are an even number of cycles of even length in its decomposition into a product of disjoint cycles.*

Proof. Indeed write $\sigma = \prod_{i=1}^{t} \sigma_i$, where the σ_i are disjoint cycles. (Actually the disjointness of the cycles is not really relevant.) Then $\epsilon(\sigma) = \prod \epsilon(\sigma_i)$. The σ_i for which $\epsilon(\sigma_i)$ is -1 are just those of even length, so for σ to be an even permutation, there must be an even number of these. ■

For example, when $n = 3$,

$$A_3 = \{1, (123), (132)\}.$$

If $n = 4$,

$$A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

We may now prove that some cube arrangements are not possible.

Theorem 11. *If $M \in \mathfrak{G}$ then $\phi_{\text{cube}}(M) \in A_{20}$.*

Proof. It is sufficient to check this for $M = U$, D, L, R, F, B since any M may be written as a product of these. If M is one of these, then $\phi_{\text{cube}}(M)$ is a product of two four-cycles, namely, an edge 4-cycle and a corner 4-cycle. Hence it is an even permutation by Theorem 10. ■

We now see why the permutations constructed in Chapter 1 were 3-cycles and not 2-cycles. We started with 3-cycles because they are the simplest constructible operations. We'd have started with 2-cycles (transpositions) if they were possible, but they are not.

Indeed $\phi_{\text{cube}}(M)$ cannot be a 2-cycle by Theorem 11. Of the cube arrangements in Figure 20, the one on the left is impossible, since it corresponds to an odd permutation (a corner transpositions). The one on the right corresponds to two transpositions, an even permutation. This does not prove that it can be constructed, but as a matter of fact it can be.

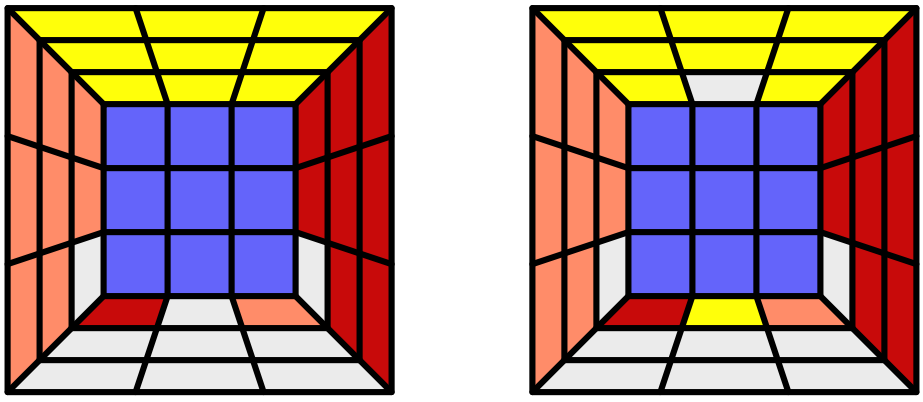

Figure 20. Left: an impossible configuration. Right: a possible one.

Here are two more impossible configurations. In Figure 17 we saw an operation that flips two edge pieces simultaneously. But it is not possible to flip a single edge piece as in the left diagram in Figure 21. Also, in Figure 18, we saw an operation that twists two corners simultaneously. But it is not possible to twist a single corner indepenedently as in the second diagram in Figure 21.

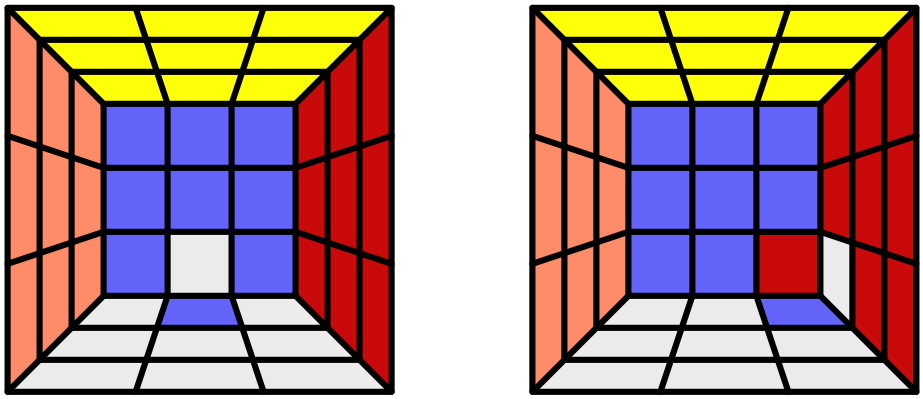

Figure 21. Impossible configurations. Left: one edge flipped. Right: one corner twisted.

Proposition 15. *The configuration in the left diagram in Figure 21 cannot be achieved.*

Proof. We can't use $\phi_{\text{edge}} : \mathfrak{G} \to S_{12}$, because the 12 edge pieces are not moved in this diagram. However we may create a modified homomorphism $\phi_{\text{edgefacelet}} : \mathfrak{G} \to S_{24}$ which does the job. Specifically, each edge piece can be thought of as a pair of *edge facelets*, and the 24 edge facelets are permuted by the motions of the cube. If $M \in \mathfrak{G}$ then $\phi_{\text{edgefacelet}}(M) \subseteq A_{24}$. Indeed, it is sufficient to check this when $M = U$, D, L, R, F, B, and indeed, in which case $\phi_{\text{edgefacelet}}(M)$ consists of a pair of 4-cycles, an even permutation. On the other hand the edge facelet permutation in the diagram in question consists of a single transposition, an odd permutation, and this permutation is therefore not $\phi_{\text{edgefacelet}}(M)$ for any $M \in \mathfrak{G}$. ∎

The impossibility of the configuration in the right diagram of Figure 21 must be proved by a different method. We will do this in the next Chapter.

Finally, we return to the point raised in the first Chapter, in the theorem Proposition 1. We prove now a related result for the symmetric group. If $\sigma \in S_n$ define the *support* $\text{supp}(\sigma)$ of σ to be $x \in X = \{1, 2, 3, \cdots, n\}$ such that $\sigma(x) \neq x$. Applying σ^{-1} to this inequality shows that $x \neq \sigma^{-1}(x)$ so

$$\text{supp}(\sigma) = \text{supp}(\sigma^{-1}).$$

Proposition 13. *Let σ, $\tau \in S_n$. Then $[\sigma, \tau] \in A_n$.*

Proof. Since $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism,

$$\epsilon([\sigma, \tau]) = [\epsilon(\sigma), \epsilon(\tau)].$$

On the right side, the commutator is computed in the abelian group $\{\pm 1\}$, so $\epsilon([\sigma, \tau]) = 1$ and therefore $[\sigma, \tau] = 1$. ∎

Proposition 14. *Let $\sigma, \tau \in S_n$. Suppose that*

$$\text{supp}(\sigma) \cap \text{supp}(\tau) = \{x\}$$

consists of a single element. Then $[\sigma, \tau]$ is a 3-cycle.

Proof. First let us show that the support of $[\sigma, \tau]$ is contained in the 3-element set $\{x, \sigma(x), \tau(x)\}$. Indeed, if $z \notin \{x, \sigma(x), \tau(x)\}$ let us show that z is fixed by $[\sigma, \tau]$. There are three cases.

First suppose that $z \notin \text{supp}(\sigma)$ and $z \notin \text{supp}(\tau)$. Neither σ nor τ (nor their inverses) affects z so $[\sigma, \tau](z) = z$.

Next suppose that $z \in \text{supp}(\sigma)$ but $z \notin \text{supp}(\tau)$. Then $\sigma^{-1}(z) \in \text{supp}(\sigma)$ but $\sigma^{-1}(z) \neq x$. Since $\{x\} = \text{supp}(\sigma) \cap \text{supp}(\tau)$, this means that $\sigma^{-1}(z) \notin \text{supp}(\tau)$. Therefore

$$[\sigma, \tau](z) = \sigma\tau\sigma^{-1}\tau^{-1}(z) = \sigma\tau\sigma^{-1}(z) = \sigma\sigma^{-1}(z) = z.$$

The last case is that $z \notin \text{supp}(\sigma)$ but $z \in \text{supp}(\tau)$. This is similar to the case just done so we leave this case to the reader.

Now we know that at most 3 elements of $X = \{1, 2, \cdots n\}$ are affected by $[\sigma, \tau]$. At least one of them is, since it is easy to check that $x \in \text{supp}[\sigma, \tau]$. Now $[\sigma, \tau]$ is in the alternating group by Proposition 13. And any permutation which affects at most three elements of X is either a 2-cycle or a 3-cycle. And $[\sigma, \tau]$ can't be a 2-cycle because it's in A_n. So it's a 3-cycle. ■

This result partially explains the fact discussed in Section 1 to the effect that if the support of two cube operations overlaps in exactly one piece, then their commutator is a 3-cycle.

Chapter 4: Modular Arithmetic

A group, as we have seen, is an algebraic structure involving only one composition law, which may be thought of as an addition, or sometimes a multiplication. A *ring* is an algebraic structure involving both an addition and a multiplication. Suppose R is a set with $+$ and $\times$ defined. As usual, $x \times y$ is often denoted just $x \cdot y$ or xy. Then R is a *ring* if certain axioms are satisfied. With respect to addition, R must be an abelian group, so it has a distinguished element 0. It has another distinguished element called 1 such that $1 \cdot x = x \cdot 1 = x$ for all $x \in R$, and the associative law $(xy)z = x(yz)$ must be satisfied. We also assume that $0 \cdot x = x \cdot 0 = 0$ for all x, and the distributive laws $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$.

If the multiplication of R is commutative, that is, $xy = yx$ for all $x \in R$, then R is called a *commutative* ring.

Note that R is not a group under multiplication, because inverses may not exist. In fact, 0 does not have an inverse unless $1 = 0$ and R consists of a single element. But if the nonzero elements of R form a group under multiplication then R is called a *division ring*. The most commonly encountered division rings are commutative, and a commutative division ring is called a *field*.

The integers $\mathbb{Z}$ are a ring which is not a field. The rational numbers $\mathbb{Q}$ and complex numbers $\mathbb{C}$ and the real numbers $\mathbb{R}$ are all fields. All of these rings are commutative. But the $n \times n$ matrices over a ring R form a ring $\mathrm{Mat}_n(R)$ which is *not* commutative if $n > 1$. The quaternions $\mathbb{H}$ are an example of a division ring which is not a field.

Let N be a fixed positive integer. The integers modulo N can be defined as follows. As a set, $\mathbb{Z}_N = \{0, 1, 2, \cdots N - 1\}$. We define the addition and multiplication in $\mathbb{Z}_N$ as follows. If a, $b \in \mathbb{Z}_N$ then $a + b$ is the remainder on division by N of their usual sum in $\mathbb{Z}$, and ab is the remainder on division by N of their usual product in $\mathbb{Z}$.

For example, in $\mathbb{Z}_3 = \{0, 1, 2\}$ the addition and multiplication are as in the following table:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

This ring has all the usual properties of arithmetic, such as the additive and multiplicative associative laws, the distributive law $a(b + c) = ab + ac$ and so forth. Similarly there is a ring $\mathbb{Z}_n$ of integers modulo n for any n. Actually we will only need the additive structure of $\mathbb{Z}_3$. But later we'll use the integers modulo 5 in a similar proof, and we'll use *both* the additive and multiplicative structures.

The ring $\mathbb{Z}_n$ is a field if n is prime, but not otherwise.

Proposition 15. *The configuration in the right diagram in Figure 21 cannot be achieved.*

Proof. Label the 24 corner facelets of the cube with numbers from $\mathbb{Z}_3$ as follows. Each of the 8 corner facelets of the up and down faces is labelled 0. The remaining 16 facelets are labelled by the requirement that as one proceeds clockwise around the three facelets in any corner piece, the numbers 0, 1 and 2 appear in sequence (Figure 23).

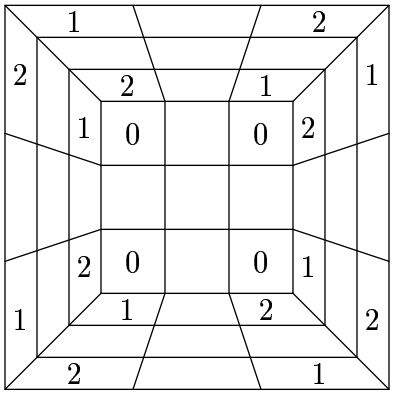

Figure 23. Mod 3 labelling of the corner facelets. Hidden facelets labelled 0.

We note that in the initial configuration (Figure 23), the sum of the eight values on any two opposite faces is zero (mod 3). We will show that as the cube is worked, that property remains true. Let us look at a single face. For simplicity, we look at the top face but the same reasoning would apply to any other.

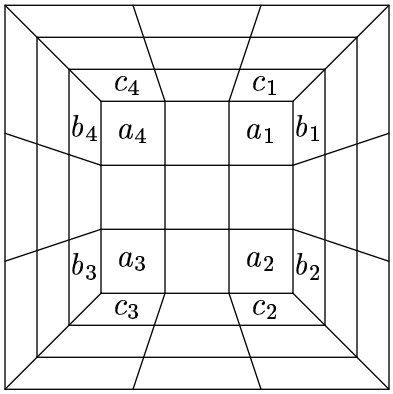

Figure 23. Facelets around a single face.

The crucial thing to observe is that

$$\sum_{i=1}^{4} b_i = \sum_{i=1}^{4} a_i = \sum_{i=1}^{4} c_i.$$

Indeed, modulo 3,

$$b_1 = a_1 + 2, \qquad b_2 = a_2 + 1, \qquad b_3 = a_3 + 2, \qquad b_4 = a_4 + 1, \tag{15}$$

and since $1 + 2 + 2 + 1 = 0$ modulo 3, we get $\sum_{i=1}^{4} a_i = \sum_{i=1}^{4} b_i$; the other equality is proved the same way.

Now rotate the top face. The sum of the values of the facelets on the top and bottom faces of course does not change. For the sum of the values of the facelets on the left and right faces, the b facelets are replaced by the c facelets, so the sum of the values of the facelets on the left and right faces is unchanged by (15). Similarly the sum of the values on the front and back faces is unchanged.

Now the right diagram in Figure 21 cannot be achieved, because the sum of the values on the top and bottom faces is 1, not 0. ■

Exercise. *Give a proof of the impossibility of the left diagram in Figure 21 (Proposition 15) different from the proof given in Chapter 3, based on ideas similar to those in the proof of Proposition 15, but using arithmetic modulo 2.*

Chapter 5: Conjugation

The operation of conjugation is fundamental in group theory. We can get some intuition about its nature by contemplating conjugacy in the symmetric groups and in the group $\mathfrak{G}$ of the Rubik's cube.

To begin with, let $g = RUR^{-1}URU^2R^{-1}L^{-1}U^{-1}LU^{-1}L^{-1}U^2L$. As we saw in Figure 18, this operation twists the upper top left front and back corners. Knowing this, if h is any element of $\mathfrak{G}$, then hgh^{-1} will twist some pair of corners. Which particular pair depends of course on h. To see how this works, consider the example $h = B$. Then the effect of $hgh^{-1} = BgB^{-1}$ is shown in Figure 19. The top front left and top back right corners are twisted.

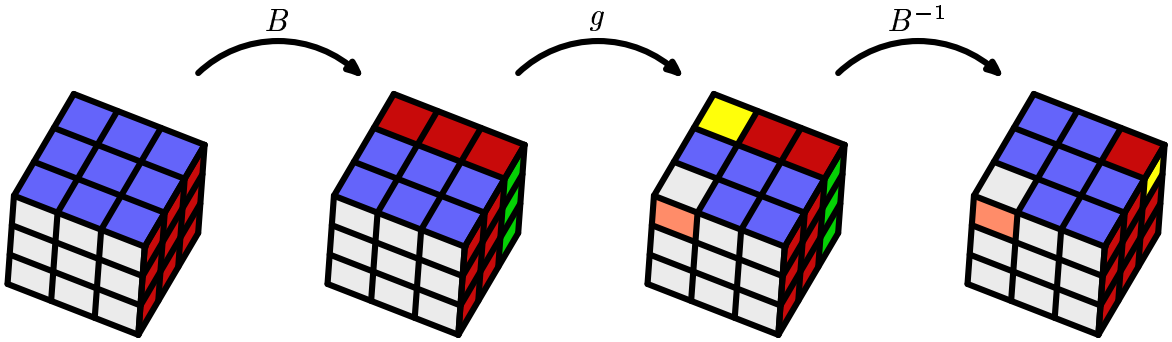

Figure 24. How conjugation works.

Figure 24 shows the mechanism by which this is accomplished. The operation g will twist two particular corners. Since instead of twisting the top back left corner we want to twist the top back right corner, we preceed the operation g by the operation B, which moves the corner we *want* to twist into the position where it *will* be twisted. And following the operation g by B^{-1} moves that piece back into its original position.

Now let us consider conjugation from a more abstract point of view. Let X be a set. Let $\sim$ be a relation on X, that is, for every x and $y \in X$, the symbol $x \sim y$ is either true or false. Then $\sim$ is an *equivalence relation* if it satisfies three axioms:

Reflexive. For all $x \in X$, we have $x \sim x$.

Symmetric. For all $x, y \in X$, $x \sim y$ if and only if $y \sim x$.

Transitive. For all $x, y, z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$.

Proposition 16. *Suppose that $\sim$ is an equivalence relation on X. For $x \in X$, define $c(x)$ to be $\{y \in X | y \sim x\}$. If x, $y \in X$ then either $c(x) \cap c(y) = \{\}$ (the empty set) or $c(x) = c(y)$.*

The set $c(x)$ is called the *equivalence class* of x. Thus X is partitioned into disjoint equivalence classes.

Proof. If $c(x) \cap c(y)$ is nonempty, say $z \in c(x) \cap c(y)$, then $x \sim z$ and $z \sim y$, so $x \sim y$ and this implies $c(x) = c(y)$. ∎

Let G be a group and x, $y \in G$. We say that x and y are *conjugate* in G, and write $x \sim y$ if there exists a $g \in G$ such that $gxg^{-1} = y$.

Proposition 17. *Conjugacy is an equivalence relation.*

Proof. Reflexive: $gxg^{-1} = x$ if $g = 1$ so $x \sim x$. Symmetric: if $x \sim y$ then $y = gxg^{-1}$ for some g, so $x = g^{-1}xg$. Transitive: if $x \sim y$ and $y \sim z$ then $y = gxg^{-1}$ for some g and $z = hyh^{-1}$. Thus $z = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}$ so $z \sim x$. ∎

If $x \in G$ then the equivalence class of x under the operation of conjugacy is called the *conjugacy class* of x. We can describe the conjugacy classes in S_n very explicitly.

First let us work out an example, in S_5. Let us conjugate $x = (12)(34)$ by $g = (12345)$.

$$gxg^{-1} = (12345)(12)(34)(15432) = (23)(45).$$

This permutation has the same shape or *cycle structure* as the original permutation $(12)(34)$. By this we mean that the two permutations $(12)(34)$ and $(23)(45)$, in their representations as products of disjoint cycles, have the same number of cycles of each length—in this case, two cycles of length two, and no cycles of any other length.

If we consider more generally

$$\sigma(12)(34)\sigma^{-1}, \qquad \sigma \in S_n,$$

first σ^{-1} sends $\sigma(1)$ and $\sigma(2)$ to 1 and 2, then $(12)(34)$ interchanges them, then σ sends them back to $\sigma(2)$ and $\sigma(1)$. Similarly this permutation interchanges $\sigma(3)$ and $\sigma(4)$. So if $\sigma(1) = a$, $\sigma(2) = b$, $\sigma(3) = c$ and $\sigma(4) = d$, then

$$\sigma(12)(34)\sigma^{-1} = (ab)(cd). \tag{16}$$

We see that the cycles conjugate to $(12)(34)$ are *precisely* the ones with the same cycle structure, and this phenomenon is completely general.

Theorem 18. *Two elements of S_n are conjugate if and only if they have the same cycle structure.*

Proof. If you understood the proof of (16), this is obvious. Indeed, if g and h have the same cycle structure, we can find a permutation σ which takes the elements of each cycle in g to a corresponding cycle of h, and in the same order. Then just as in (16) we have $\sigma g \sigma^{-1}$. ∎

We caution the reader that this fact fails in A_n. For example in S_3, (123) and (132) are conjugate, indeed $(12)(123)(12)^{-1} = (132)$. But A_3 is commutative, so (123) and (132) are *not* conjugate in A_3, even though they are both even permutations.

As examples, here are the conjugacy classes in S_3:

$$\{1\}, \qquad \{(12), (13), (23)\}, \qquad \{(123), (132)\}.$$

Here are the conjugacy classes in S_4:

$$\{1\}, \qquad \{(123),(132),(124),(142),(134),(143),(234),(243)\},$$

$$\{(12)(34),(13)(23),(14)(23)\}$$

$$\{(1234),(1243),(1324),(1342),(1423),(1432)\},$$

$$\{(12),(13),(14),(23),(24),(34)\}.$$

Now this same phenomenon should apply to the Rubik's cube. If we conjugate a corner three cycle, we should get another corner three cycle, and if we conjugate a corner edge cycle, we should get another corner edge cycle. This is a fact of great practical utility since it allows us to construct new operations from old ones. We consider an example.

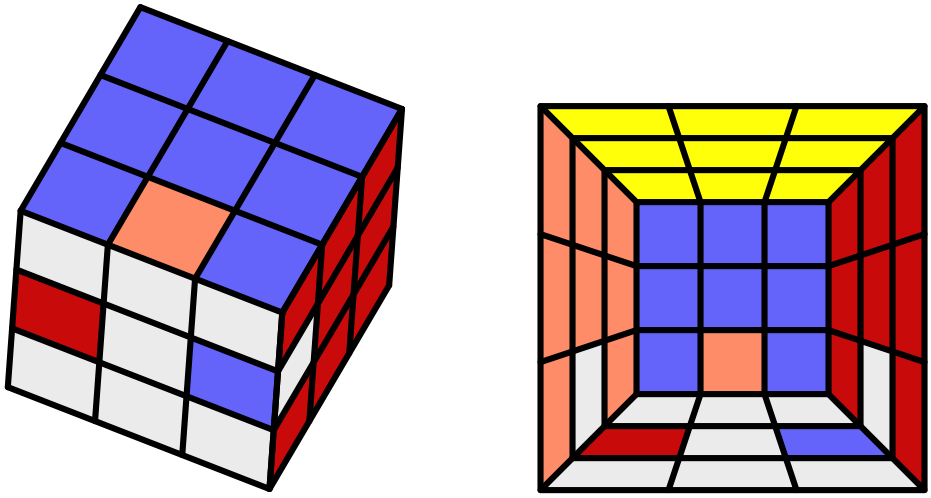

Figure 25. An edge 3-cycle $RU^{-1}RU_{\mathrm{m}}^{-1}RUR^{-1}U_{\mathrm{m}}$.

As the reader of Chapter 1 will understand, three particular edge 3-cycles are

$$RU^{-1}RU_{\mathrm{m}}^{-1}RUR^{-1}U_{\mathrm{m}}, \qquad RU^{-1}RU_{\mathrm{m}}^{2}RU^{2}R^{-1}U_{\mathrm{m}}, \qquad RU^{-1}RU_{\mathrm{m}}RUR^{-1}U_{\mathrm{m}}^{-1},$$

These are commutators $[RU^{-1}R^{-1}, U_{\mathrm{m}}^{k}]$ for various powers of k, and they work because U_{m} and $RU^{-1}R^{-1}$ only affect one vertex in common.

For example the first of these operations is shown in Figure 25.

Now let's use the conjugation principle to construct another *different* cube operation which affects exactly the same three edges. We start with the operation in Figure 26.

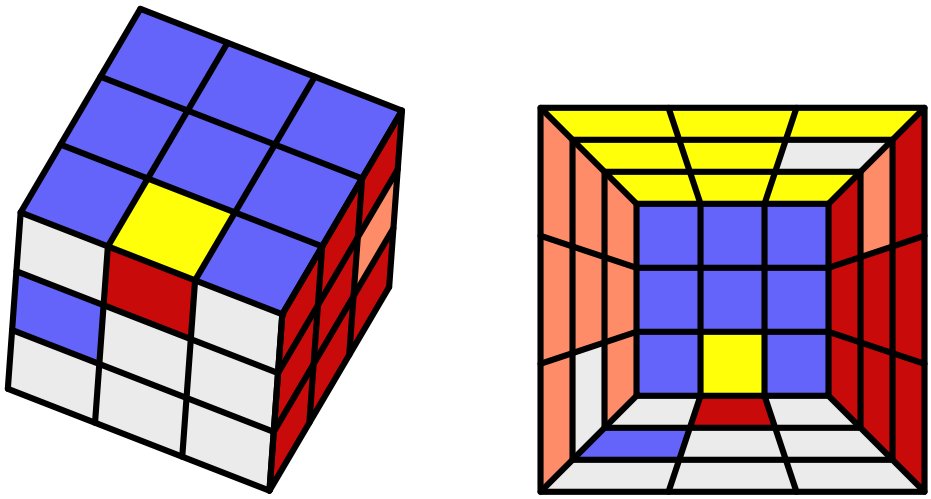

Figure 26. Another edge 3-cycle $L^{-1}ULU_{\mathrm{m}}^2L^{-1}U^{-1}LU_{\mathrm{m}}^2$.

Remember that we are looking for an edge 3-cycle affecting the front left, right and top edges, like the one in Figure 25. The operation in Figure 26 has the right cycle type, and it affects two out of three of the right edge pieces. If we *conjugate* it by R^2, which interchanges the right back edge for the right front edge, then we will get an edge three cycle with exactly affecting the three desired pieces. This is just like (16). Indeed, this operation is $R^2(L^{-1}ULU_{\mathrm{m}}^2L^{-1}U^{-1}LU_{\mathrm{m}}^2)R^2$ (since $(R^2)^{-1} = R^2$), which has the effect in Figure 27.

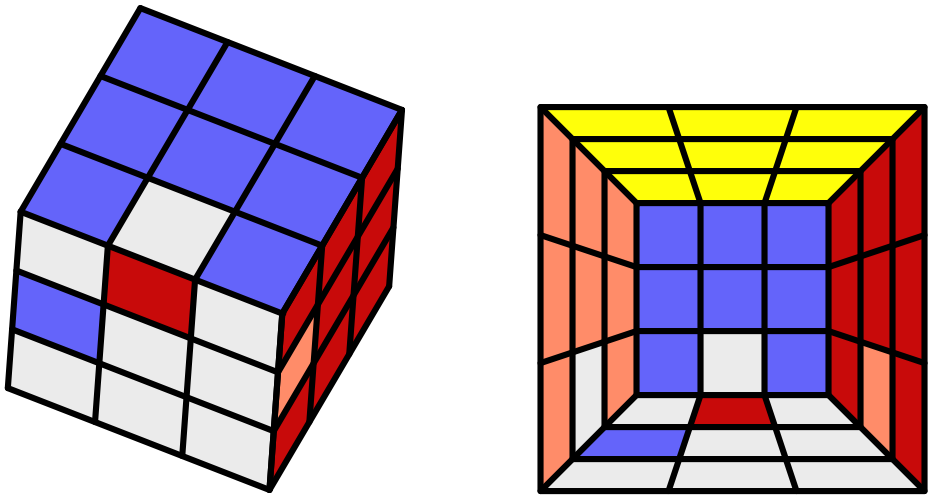

Figure 27. The conjugated edge 3-cycle $R^2(L^{-1}ULU_{\mathrm{m}}^2L^{-1}U^{-1}LU_{\mathrm{m}}^2)R^2$.

Now, let $g = RU^{-1}RU_{\mathrm{m}}^{-1}RUR^{-1}U_{\mathrm{m}}$ and $h = R^2(L^{-1}ULU_{\mathrm{m}}^2L^{-1}U^{-1}LU_{\mathrm{m}}^2)R^2$ be the two 3-cycles in Figure 25 and Figure 27. We constructed these so that they would affect the same three pieces, and *as permutations* they are inverses of each other. That is, $\phi_{\mathrm{cube}}(g)$ and $\phi_{\mathrm{cube}}(h)$ are inverses. However, as cube operations they are not inverses, and in fact gh returns the three pieces to their original position, but with two faces flipped! Indeed,

this is exactly the operation in Figure 17.

Let us give one more application of conjugation. One approach to solving the cube is to first restore the bottom, then the middle layer, and finally the top. During the final stage, one obviously wants operations which only affect the nine pieces of a single face. We begin by considering the commutator $[R, U] = RUR^{-1}U^{-1}$. This has the effect shown in Figure 28.

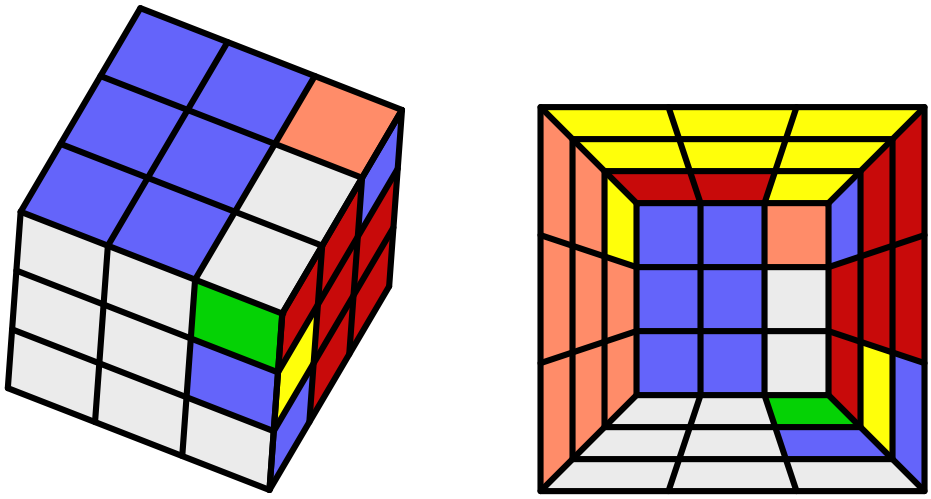

Figure 28. The commutator $[R, U] = RUR^{-1}U^{-1}$.

Note that only seven pieces are effect, all but two being in the top face. The two affected pieces not in the top row are the front left edge and front left bottom corner.

Now we can move two pieces from the top row into those positions with F, so conjugating by F should give an operation affecting only the top row! See Figure 29.

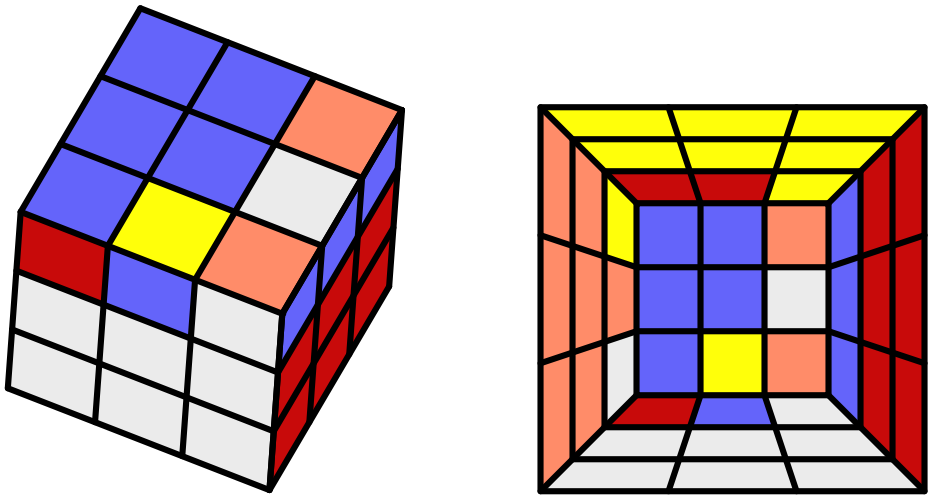

Figure 29. The conjugated commutator $F[R, U]F^{-1} = FRUR^{-1}U^{-1}F^{-1}$.

The effect of this operation is somewhat complicated, so let us consider how it might be applied. First of all, let us consider exactly what it does. The top front corners

are switched, and so are the top back corners. So the cycle type of $\phi_{\text{corner}}(F[R,U]F^{-1})$ is (12)(34). On the other hand the effect on the edge pieces is that of a 3-cycle, the top left edge not moving, and the other top three edges being permuted cyclicly. So $\phi_{\text{edge}}(F[R,U]F^{-1})$ has the cycle type (123).

For some purposes, ϕ_{corner} or ϕ_{edge} might be irrelevant. Suppose, for example, that we have solved the bottom and middle layers of the cube and the task that confronts us is to do the top layer. We have a choice of either doing the corners first, or the edges first. If we decide to do the corners first, then we do not care whether our operations affect the top edges or not. So if ϕ_{corner} does what we want, the effect of ϕ_{edge} is irrelevant.

Let us consider what happens when we raise the operation $F[R,U]F^{-1}$ to a power. As a special case of (4),

$$(hgh^{-1})^n = hg^nh^{-1}.$$

This means that squaring or cubing $F[R,U]F^{-1}$ gives

$$F(RUR^{-1}U^{-1})^2F^{-1} \qquad \text{or} \qquad F(RUR^{-1}U^{-1})^3F^{-1}.$$

Such an operation is easy to do quickly. But is it useful? Yes, potentially.

Since $\phi_{\text{corner}}([R,U])$ is a pair of 2-cycles, $F[R,U]^2F^{-1}$ will leave the corners in their original positions. As it turns out, they get twisted (Figure 30, left). This could be a useful effect. Cubing on the other hand puts the edge pieces aright but leaves the corners switched.

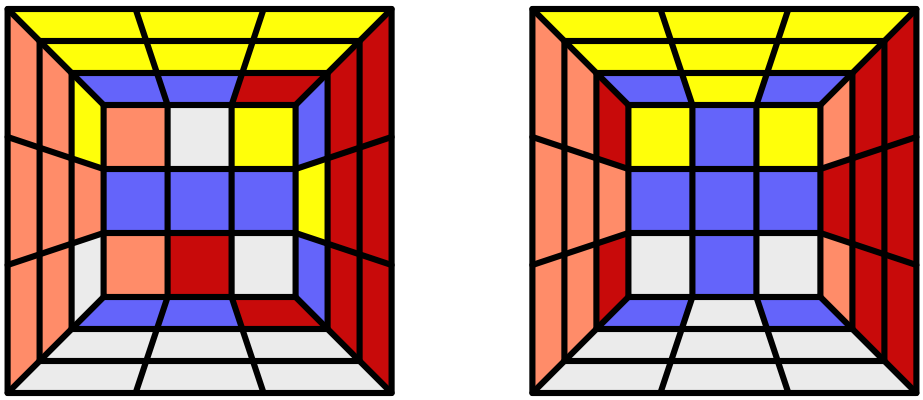

Figure 30. Left: $F[R,U]^2F^{-1}$. Right: $F[R,U]^3F^{-1}$

Chapter 6: Group Actions

If G is a group and X is a set, a *group action* of G on X is a rule that associates, for every $g \in G$ and $x \in X$ an element $g \cdot x \in X$. The action must satisfy the associative law $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$, and $1 \cdot x = x$. As an example, the symmetric group S_n acts on the set $N = \{1, 2, 3, \cdots, n\}$, indeed if $g \in S_n$ then g is a mapping $N \to N$ and we define $g \cdot x = g(x)$.

As another example, let G be any group, let $X = G$ and define

$$g \cdot x = gxg^{-1} \tag{17}$$

It may easily be checked that this is a group action.

Again, let $G = S_4$ acting on $N = \{1, 2, 3, 4\}$. Let X be the set of three pairs of subsets of N,

$$a = \{\{1, 2\}, \{3, 4\}\},$$

$$b = \{\{1, 3\}, \{2, 4\}\},$$

$$c = \{\{1, 4\}, \{2, 3\}\}.$$

Then G acts on $\{a, b, c\}$. For example (12) applied to a does not change it, but (12) interchanges b and c, so

$$(12) \cdot a = a, \qquad (12) \cdot b = c, \qquad (12) \cdot c = b.$$

Given a group action of G on a finite set X with k elements amounts to a homomorphism $\phi : G \to S_k$, where we regard the symmetric group S_k as the group of permutations of X. Indeed, given such a group action, we may identify X with $\{1, 2, \cdots, k\}$, then define

$$\phi(g) : X \to X, \qquad \phi(g)(x) = g \cdot x. \tag{18}$$

In the last example, we are regarding S_3 as the group of permutations of $\{a, b, c\}$, and we get a homomorphism $\phi : S_4 \to S_3$ with $\phi(12) = (bc)$. This example is interesting because homomorphisms from large symmetric groups to smaller ones are fairly rare.

Exercise. *The kernel of this homomorphism is a subgroup V of S_4. Find its elements.*

Conversely, if we are given a homomorphism from $\phi : G \to S_k$, where S_k acts on a set X with k elements, then we have an action of G on X defined by

$$g \cdot x = \phi(g)x. \tag{19}$$

Exercise. *Prove that (19) defines a group action.*

So group actions (at least on finite sets) and homomorphisms into symmetric groups are closely related concepts.

Again, let G be a group and H a subgroup. Then H acts on G by $h \cdot x = hx$ ($x \in G$, $h \in H$). This action is called *left translation*. We could define a different action, called *right translation* by $h \cdot x = xh^{-1}$. (The inverse is necessary to make the associative law true.)

If G acts on X (that is, if a group action of G on X is specified) then define $x_1 \sim x_2$ for $x_1, x_2 \in X$ if $x_1 = g \cdot x_2$ for some $g \in G$. It is easy to see that $\sim$ is an equivalence relation. The equivalence classes are called the *orbits* of G on X. Thus in the action of G on itself by conjugation, the orbits are conjugacy classes.

Proposition 19. *Let G act on X. Then X is the disjoint union of the orbits of G on X.*

Proof. Since $x_1 \sim x_2$ is an equivalence relation, this follows from *Proposition* 16. ■

Let H be a subgroup of G, and let $x \in G$. The set $Hx = \{hx | h \in H\}$ is called a *right coset of H*. As you can see, it is an orbit of H in the action of H on G by left translation.

Proposition 20. *Let H be a subgroup of G. Then G is the disjoint union of the right cosets Hx.*

Proof. This is a special case of Proposition 19. ■

The *order* of a group G is its cardinality, that is, the number of elements in G. (It may be infinite though we'll encounter mainly finite groups due to our subject matter.) We denote the order of G by $|G|$. More generally we denot the number of elements of a (usually finite) set X by $|X|$.

If $x \in G$ then the group *generated* by x is $\langle x \rangle = \{x^n | n \in \mathbb{Z}\}$. (More generally if G is a group and S a subset, the subgroup $\langle S \rangle$ *generated* by S is the smallest subgroup of G containing S. For example group $\mathfrak{G}$ is generated by $\{U, D, L, R, F, B\}$. A group is called *cyclic* if it is generated by a single element. We denote the cyclic group generated by $g \in G$ as $\langle g \rangle$, and its order by $|g|$.

Proposition 21. *Let G be a finite group and H a finite subgroup. Then $|H|$ divides $|G|$.*

Proof. Each coset Hx has the same number $|H|$ of elements as H itself. Indeed $h \to hx$ is a bijection $H \to Hx$. Since by Proposition 20, G is the disjoint union of its right cosets, and these have the same size $|H|$, it follows that $|H|$ must divide G. ■

If H is a subgroup of G, then we denote the number of right cosets Hx by $[G : H]$. It is called the *index* of H in G. It follows from Proposition 21 that if G and H are finite then $[G : H] = |G|/|H|$. However the notion of index makes sense, and may be finite, even of G and H are infinite. For example if G is the group $\mathbb{Z}$ of integers (group law addition) and H is the subgroup of even integers, then G and H are both infinite but $[G : H]$ is just 2.

Exercise. *(i) Let G be a group and H a subgroup. Prove that*

$$Hx \to x^{-1}H$$

is a bijection between the right cosets of H and the left cosets.
(ii) Explain why we used $x^{-1}H$ and not xH.

We let G/H be the set of left cosets xH of H in G.

If G acts on a set X and $x_0 \in X$, the *isotropy subgroup* or *stabilizer* of x_0 is the subgroup

$$H_{x_0} = \{g \in G | gx_0 = x_0\}.$$

Exercise. *Suppose that G acts on X and let $x_0, y_0 \in X$. If x_0 and y_0 are in the same orbit, prove that the isotropy groups H_{x_0} and H_{y_0} are conjugate, that is, $gH_{x_0}g^{-1} = H_{y_0}$ for some $g \in G$.*

Hint: Find g such that $g \cdot x_0 = y_0$.

If G acts on a set X, the action is *transitive* if G has only one orbit. This means that if $x, y \in X$ then $y = g \cdot x$ for some $g \in G$.

Proposition 22. *Let G be a group acting transitively on X. Let $x_0 \in X$ be some fixed element, and let $H = H_{x_0}$ be its isotropy subgroup. Then X is in bijection with G/H.*

Proof. Because the group action is transitive, every element of X can be written as $g \cdot x_0$ for some $g \in G$. Thus it is enough to show that $g \cdot x_0 = h \cdot y_0$ if and only if the cosets xH and yH are the same. Indeed, $g \cdot x_0 = h \cdot x_0$ if and only if $x_0 = g^{-1}hx_0$, if and only if $g^{-1}h \in H$, if and only if $g^{-1}hH = H$, if and only if $hH = gH$. ∎

As a consequence, we have

$$|X| = [G : H] = |G|/|H| \tag{20}$$

Let us apply these ideas to the group of the icosahedron. The *icosahedron* is the regular Platonic solid illustrated in Figure 31. We consider the group G_{icosa} of rotations mapping it into itself.

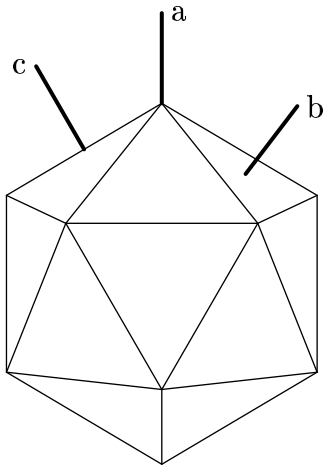

Figure 31. The Icosahedron.

We can use 20 to determine the order of G_{icosa}. In fact, we can do this in at least three different ways. First consider the action of G_{icosa} on the set X of vertices of the icosahedron. There are 12 such vertices, and the isotropy group H of the top vertex consists of the five rotations around the axis labelled 'a' in Figure 31. By 20 we have $|G| = |X| \cdot |H| = 12 \cdot 5 = 60$.

Alternatively, we can take X to be the set of 20 faces of the icosahedron. The isotropy group H of the top right front face consists of the three rotations around the axis labelled 'b', so $|G| = 20 \cdot 3 = 60$. Or, we can use the edges to make the same computation.

Two groups A and B are considered to have the same structure if there is a homomorphism $\phi : A \to B$ which is bijective. We say A and B are *isomorphic*. In this case, the inverse map $\phi^{-1} : B \to A$ is also a homomorphism. The relationship of being isomorphic is an equivalence relation. It means, essentially, that A and B have the same multiplication table.

Since $|G_{\text{icosa}}| = 60 = A_5$ one might wonder if they are the same group.

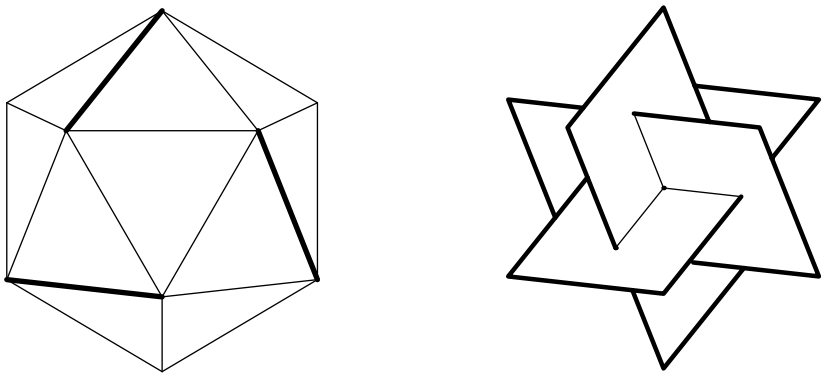

Figure 32. Three mutually perpendicular Golden Rectangles in the icosahedron.

Proposition 23. *The groups G_{icosa} and A_5 are isomorphic.*

Proof. We first exhibit a homomorphism $G_{\text{icosa}} \to S_5$ using 18 by exhibiting a set X of order 5 on which G acts. Consider the six edges consisting of the three marked ones in the left diagram in Figure 32 together with their three (hidden) opposites.

Each edge, together with its opposite form a rectangle, and the three such rectangles intersect perpendicularly in the figure in the right diagram in Figure 32. Although it is not relevant to the proof, it is interesting to note that these rectangles are so-called "Golden Rectangles," whose sides have lengths in the ratio $\frac{1+\sqrt{5}}{2} = 1.618\cdots$.

There are actually 5 such figures, each consisting of three mutually perpendicular Golden Rectangles whose vertices coincide with those of the icosahedron. The the group of the icosahedron acts on this set of 5 figures. Thus 18 gives a homomorphism $G_{\text{icosa}} \to S_5$.

The reader may check that if g around an axis through a vertex (e.g. 'a' in Figure 31) then the cycle type of $\phi(g)$ is (12345); if g is a rotation through a face (e.g. 'b' in Figure 31) then the cycle type (123); and if of $\phi(g)$ is (12345); if g is a rotation through a edge (e.g. 'c' in Figure 31) then the cycle type of $\phi(g)$ is (12)(34). In every case, $\phi(g)$ is nontrivial and is in A_5, so the kernel of ϕ is trivial (hence by Proposition 2, ϕ is injective) and $\phi : G_{\text{icosa}} \to A_5$. Since both groups have the same order, ϕ must be an isomorphism. ■

Exercise. *Use similar considerations to show that that the group of rotations of the tetrahedron has order* 12 *and is isomorphic to* A_4*, and that the group of rotations of the cube has order* 24 *and is isomorphic to* S_4*. How about the octahedron and dodecahedron?*

If G is a group and $g \in G$ the set

$$C_G(g) = \{h \in G | hg = gh\}$$

of elements which commute with g is clearly closed under multiplication and inverses, hence is a subgroup of G.

As a final example of the ideas in this Chapter, we let G act on itself by conjugation, that is, (17). The orbits are just the conjugacy classes. Thus we obtain:

Proposition 24. *Let* G *be a finite group, and let* $g \in G$*. Then the number of elements of the conjugacy class of* g *divides* $|G|$*, and equals the index of* $C_G(g)$*.*

Proof. The group G acts on the single conjugacy class X of G, and by definition of a conjugacy class, this action is transitive. The isotropy subgroup of g consists of $\{h | hgh^{-1} = g\}$, which is clearly the same as $C_G(g)$. ■

Exercise. *List the conjugacy classes of* S_5 *and compute their orders. Describe the centralizer of each element and confirm Proposition 24. There should be 7 cases.*

Exercise. *(a) Let* G *be a group acting on a set* X*. Let* $x_0 \in X$ *and let* H *be the stabilizer of* x_0*. Let* S *be a subset of* G*. Suppose that the group generated by* S *contains the* H*, and is transitive on* X*. Prove that* S *generates* G*.*

(b) Let S *be the set consisting of the rotations around the axes* a *and* b *in Figure 31. Show that these generate* G_{icosa}*.*

Chapter 7: Normal Subgroups

If G is a group and N is a subgroup, and if $g \in G$, we naturally denote by gNg^{-1} the set of all gng^{-1} such that $n \in G$. The subgroup N is called *normal* if $gNg^{-1} = N$ for all $g \in G$. We can express this by saying that N is invariant under conjugation.

Lemma 25. *If $gNg^{-1} \subset N$ for all $g \in G$ then N is normal.*

Proof. We must show that $N \subset gNg^{-1}$. Since we are assuming that $gNg^{-1} \subset N$ for all $g \in G$, this remains true when g is replaced by g^{-1}. Thus $g^{-1}Ng \subset N$, and multiplying this relation on the left by g and on the right by g^{-1} gives $N \subset gNg^{-1}$. ■

For example, if $G = S_3$, the subgroup $N = \langle (123) \rangle = \{1, (123), (132)\}$ is normal, since it is a union of two conjugacy classes, 1 and $\{(123), (132)\}$. So it is invariant under conjugation.

On the other hand, if again $G = S_3$, the subgroup $H = \langle (12) \rangle$ is not normal, because if $g = (123)$ then $gHg^{-1} = \langle (23) \rangle \neq H$.

Proposition 26. *Let $\phi : G \to H$ be a homomorphism of groups. Then the kernel K of ϕ is normal.*

Proof. We must show for every $g \in G$ that $gKg^{-1} \subset K$. In other words, if $k \in K$ we must show that $gkg^{-1} \in K$. Since $k \in K$ we have $\phi(k) = 1$. Now

$$\phi(gkg^{-1}) = \phi(g)\,\phi(k)\,\phi(g)^{-1} = \phi(g) \cdot 1 \cdot \phi(g)^{-1} = 1.$$

This shows that $gKg^{-1} \subset K$ so K is normal in G. ■

The alternating group A_n is a normal subgroup of S_n. Indeed, it is the kernel of the homomorphism $\epsilon : S_n \to \{\pm 1\}$ constructed in Chapter 3.

We constructed a homomorphism $S_4 \to S_3$ in Chapter 6 whose kernel is therefore a normal subgroup V of order 4. But it can be proved that the *only* case where S_n (for any n) has a normal subgroup other than $\{1\}$, S_n itself, and A_n.

A group G is called *simple* if its only normal subgroups are $\{1\}$ and G itself. Simple groups are important because in a sense (which we will not explain) they are the basic building blocks of groups. The finite simple groups have been classified, around 1980 (work of many).

Proposition 27. *The group A_5 is simple.*

Proof. Suppose that H is a normal subgroup of A_5. Then the order $|H|$ divides 60. Moreover if H contains an element of one conjugacy class of A_5, it contains the whole conjugacy class, because H is normal.

We compute easily the conjugacy classes in A_5. They are the conjugacy classes of 1, (12345), (13524), (123) and (12)(34), having orders 1,12,12,20 and 15 respectively. This $|H|$ is a divisor of 60, whose order is a sum of some of $\{1, 12, 12, 20, 15\}$. And at least one of the conjugacy classes contained in H is $\{1\}$, so we can say more precisely that $|H|$ equals 1 plus some of $\{12, 12, 10, 15\}$. It can be checked quickly that the only divisors of 60 which can be expressed as a sum of 1 and some of $\{12, 12, 20, 15\}$ are 1 and 60. So either $H = \{1\}$ or $H = A_5$. ■

On the other hand A_4 is not simple, because it contains the normal subgroup V. But A_4 is the only alternating group which is not simple. (We will not prove this.)

The abelian simple groups are easy to construct. Any subgroup of an abelian group is automatically normal, so an abelian simple group is a group G with no subgroups at all except 1 and G. It is easy to see that such a group is a cyclic group of prime order.

On the other hand A_5 is the smallest nonabelian simple group. (A_3 is simple but abelian.) It can be shown that A_n is simple for any $n \neq 4$. This gives an infinite family of nonabelian simple groups.

We've seen that the kernel of a homomorphism is a normal subgroup. Conversely, we will next show that any normal subgroup is the kernel of a homomorphism.

Let N be a normal subgroup of G. If $g \in G$ then $gNg^{-1} = N$, and multiplying on the right by g gives $gN = Ng$. So the left and right cosets of G are the same. Let G/N be the set of cosets.

If X, Y are subsets of G, we naturally denote by XY the set of all products xy with $x \in X$ and $y \in Y$, and we will use similar such notations for products of sets and elements of g. Thus for example if gN and $hN \in G/N$, then $gNhN$ denotes the set of all $gnhn'$ such that $n, n' \in N$. We note that (using the normality of N)

$$gN\,hN = gh(h^{-1}Nh)N = ghN \cdot N = ghN. \tag{21}$$

Thus the product of two cosets is a coset.

Proposition 28. *If N is normal in G, then G/N is a group and $\pi : G \to G/N$ defined by $\pi(g) = gN$ is a homomorphism. It's kernel is N.*

Proof. It follows from (21) that the multiplication of cosets is a well defined associative composition law and that $N = 1N$ acts as an identity element. Moreover, taking $h = g^{-1}$ in (21) shows that $g^{-1}N$ is an inverse of gN. Moreover (21) shows π is a homomorphism. Since $gN = N$ if and only if $g \in N$ the kernel is N. ■

We now see that the normal subgroups are exactly the ones that can be kernels of homomorphisms.

If G is any group, the *center* $Z(G)$ consists of all $g \in G$ which commute with all elements of G, that is, $gx = xg$ for all $x \in G$. It is normal. If $G = \mathfrak{G}$, the group of the Rubik's cube, then the center has order two. The nonidentity element, which we might call the *central involution* of $\mathfrak{G}$ consists of the operation which flips all edges (see Figure 33).

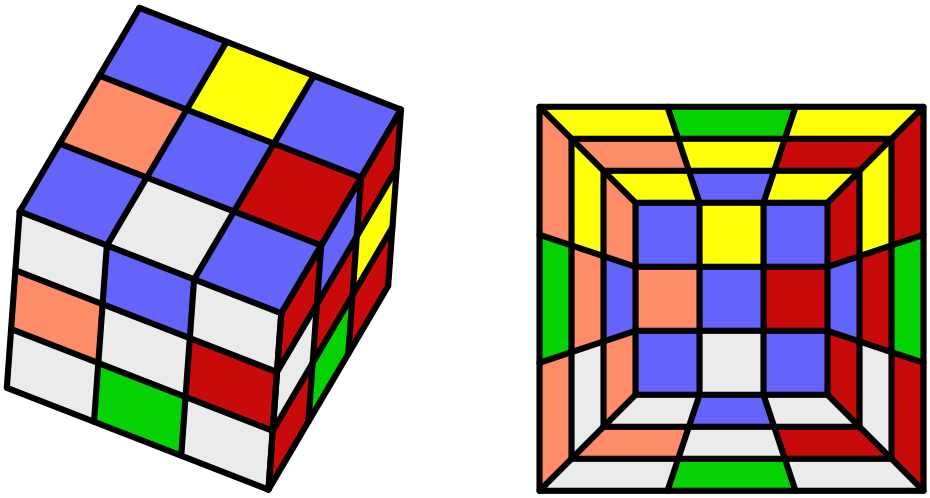

Figure 33. The effect of the central involution.

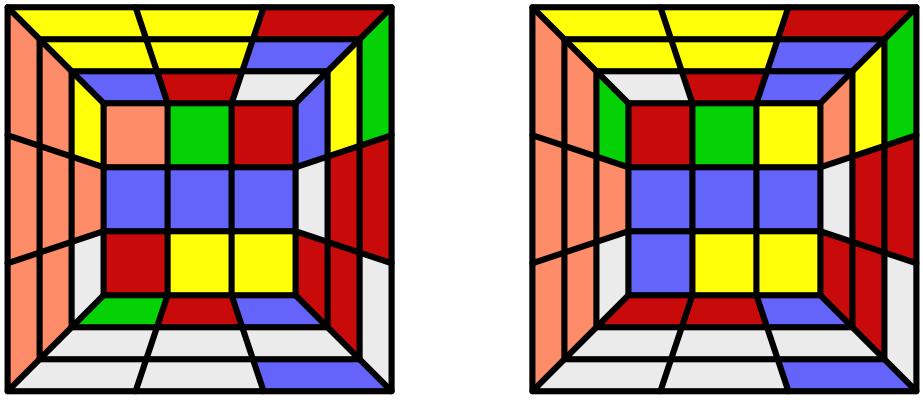

Figure 34. A possible and impossible configuration for the two generator group

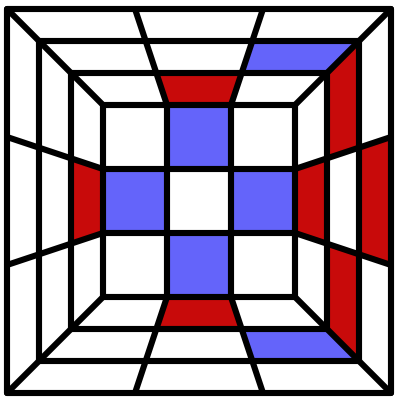

Figure 35. The possible orientations of the top right corner

Chapter 8: The two-generator group

Suppose that you scramble the cube using only two operations, R and U, then are asked to restore the cube using exactly the same two operations. This is a problem comparable in interest to the more familiar problem of restoring a scrambled cube using all operations. We will denote by $\mathfrak{T}$ the group $\langle R, U\rangle$ generated by these two operations.

One might think that the two generator problem would be harder, since in restoring the cube one is allowed only limited operations. However the universe of configurations which can be obtained using $\mathfrak{T}$ is very much limited.

The first constraint on the possible configurations is an obvious one: there are 11 pieces that never move. Thus **any achievable configuration does not move these pieces.**

However, this is not the whole story as we will explain. In Figure 34 there are two configurations which satisfy this first constraint of not moving the 11 pieces along the bottom left. Both configurations are achievable in $\mathfrak{G}$ but only the left one is achievable in $\mathfrak{T}$. Yet both look equally scrambled.

In addition to this obvious constraint, that an operation cannot move the 11 pieces along the bottom left, there there are two other constraints on the configurations which are achievable in $\mathfrak{T}$. First, with the seven edge pieces which are moved by R and U, any permutation of their locations can be achieved, but *edge flips are not possible.*

This is easy to see. If we consider the edge piece in the top left, it can be moved to 7 locations in all, but only one configuration is possible in each of these locations. The 7 possible configurations for this piece are shown in Figure 35. It is clear that from one of these configurations R and U can only move the piece into another one of the same, and so any element of the group must keep the piece in one of these configurations. It follows from this that edge flips are not possible.

There is one more, deeper constraint. We refer to the difference between the left and right configurations in Figure 34. These differ by a corner three cycle. In fact, corner three cycles are possible in $\mathfrak{G}$ but not $\mathfrak{T}$. This is a special instance of a remarkable fact about the two generator group, which is important enough for us to state it as a theorem. Let P be the set of six corners which are moved by $\mathfrak{T}$, namely the four on the right and the two top left ones.

Theorem 29. *Let g be an element of $\mathfrak{T}$, and let $\phi_{\text{corner}}(g)$ be the corresponding corner permutation. If $\phi_{\text{corner}}(g)$ fixes three elements of P then it fixes all six.*

Note that this is an assertion about the locations of the six pieces, not their orientations. For example, the operation $RUR^{-1}URU^2R^{-1}U^2 \in \mathfrak{T}$ has the effect in the left diagram in Figure 36. All the corner pieces are in their correct position though three are not in their correct orientation. Three edge pieces also are permuted in a 3-cycle.

This useful element of $\mathfrak{T}$ has order 3. (The operation in Figure 18 was built up from two operations of this type, this one and its mirror image.)

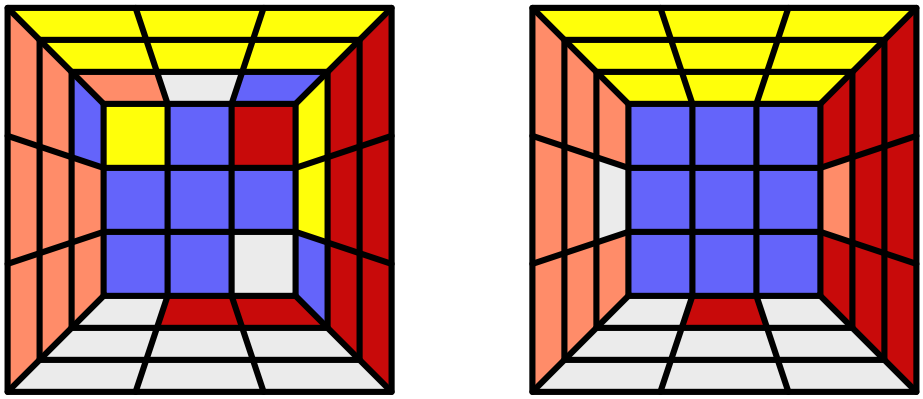

Figure 36. Left: $RUR^{-1}URU^2R^{-1}U^2$. Right: $RUR^{-1}URU^2R^{-1}U^{-1}R^{-1}U^{-1}RU^{-1}R^{-1}U^2RU$.

The implications of this Theorem for the two edge problem are important. It is simple to maneuver the two bottom corners into their correct positions and orientations. Then applying a power of U will put one more corner into its correct position, after which the Theorem asserts that all six corners are in their right places. Some of the top corners may be twisted, but applying conjugates of the operation in Figure 36 will put them right. At this point, the cube is largely solved, for only edge pieces are out of place.

In fact, one needs only edge three cycles to finish the cube. Combining the operation $RUR^{-1}URU^2R^{-1}U^2$ in the left diagram Figure 36 with a conjugate of its mirror image gives an edge three cycle. This is the operation in the right diagram of Figure 36. Together with its mirror images and conjugates, this operation is sufficient to finish the cube. Also sometimes useful is $R^2U^2R^2U^2R^2U^2$ (try it!) and its conjugates.

Chapter 9: Projective Geometry

Projective geometry was invented by Desargues (1591–1661), inspired by the theory of perspective, developed by artists and architects. Felix Klein (1849–1925) emphasized that groups play an important role in geometry, and projective geometry is a good place to see why he was right about this point.

The historical starting point of projective geometry is plane geometry. In classical Euclidean or affine geometry, the plane is $\mathbb{R}^2$ and the objects of study are geometric figures such as lines, circles or ellipses, etc. There is no real reason why geometry is only carried out over the real numbers and we can more generally consider the affine plane F^2 where F is any field, or affine n-space $\mathbb{A}^n(F) = F^n$.

In the affine plane it is *almost* true that any two lines intersect in a unique point. The exception, according to Euclid, is that *parallel* lines do not intersect. But Desargues, motivated by the artistic theory of perspective, adjoined to the affine plane a *line at infinity*. Parallel lines in the affine plane can be extended to the projective plane, and once extended they intersect on the line at infinity. Thus in projective geometry any two lines intersect in a unique point, with no exceptions. In other ways which we won't go into, the geometry of the projective plane is more perfect than affine geometry.

More generally, projective n-dimensional space consists of affine n-space with an $n-1$-dimensional projective space adjoined:

$$\mathbb{P}^n(F) = \mathbb{A}^n(F) \cup \mathbb{P}^{n-1}(F)$$

so particularly $\mathbb{P}^1(F)$ consists of the affine line with a single point at infinity, which we denote ∞: $\mathbb{P}^1(F) = F \cup \{\infty\}$.

Klein's viewpoint was that a geometry consists of a topological space X together with a group of transformation. In Euclidean or affine geometry the space $X = \mathbb{A}^n(\mathbb{R})$. There is a distinction between Euclidean and affine geometry. In Euclidean geometry the group consists of all rigid motions of $\mathbb{A}^n(\mathbb{R})$, which preserve distances and angles. In affine geometry the group is larger, adjoining transformations which preserve lines but may distort distances and angles. For example in $\mathbb{A}^2(\mathbb{R})$ the transformation

$$(x, y) \to (x + y, y)$$

is an affine transformation but not a Euclidean one, since it turns lines into lines but distorts rectangles into parallelograms.

Klein's viewpoint marked an important transition to a group-theoretic point of view in geometry, and helped clear up the 19-th century controversy over the foundations of non-Euclidean geometry.

For our purposes we will only need the projective line and its group. The group $GL(2,F)$ is the multiplicative group of 2×2 invertible matrices with coefficients in F. The group multiplication is matrix multiplication.

We have a group action of $GL(2,F)$ on $\mathbb{P}^1(F)$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}. \tag{22}$$

Such a map is called a *linear fractional transformation* or a *Möbius* transformation. There are some special cases in which this definition needs interpretation. First, if $z=\infty$, then we interpret $\frac{a\infty+b}{c\infty+d}$ to mean just $\frac{a}{c}$. Second, if $z\neq\infty$ but $cz+d=0$, then we interpret $\frac{az+b}{cz+d}$ to mean ∞.

Proposition 30. *If F is a field then (22) is an action of $GL(2,F)$ on $\mathbb{P}^1(F)$.*

Proof. Remembering that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} aA+bC & aB+bD \\ cA+dC & cB+dD \end{pmatrix}$$

we need to show that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left(\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot z \right) == \begin{pmatrix} aA+bC & aB+bD \\ cA+dC & cB+dD \end{pmatrix} \cdot z.$$

The left side is

$$\frac{a\left(\frac{Az+B}{Cz+D}\right)+b}{c\left(\frac{Az+B}{Cz+D}\right)+d.}$$

Multiplying numerator and denominator by $Cz+D$ gives

$$\frac{a(Az+B)+b(Cz+D)}{c(Az+B)+d(Cz+D)} = \frac{(aA+bC)z+(aB+bD)}{(cA+dC)z+(cB+dD)}$$

as required.

This assumes that $z\neq\infty$, $Cz+D\neq 0$ and $(aA+bC)z\neq 0$. Otherwise there are various cases to consider but in each case the identity can be checked. ■

Some elements of $GL(2,F)$ act trivially on $\mathbb{P}^1(F)$. Thus if $g=\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ then $g\cdot z = z$ for all $z\in\mathbb{P}^1(F)$. We call a matrix of this form a *scalar matrix*. The scalar matrices comprise the center of $GL(2,F)$.

Proposition 31. *If $z_1,z_2,z_3\in\mathbb{P}^1(F)$ are all distinct then there exists $g\in GL(2,F)$ such that $g\cdot z_1=\infty, g\cdot z_2=0$ and $g\cdot z_3=1$.*

Proof. First note that there is $g_1 \in GL(2,F)$ such that $g_1 \cdot z_1 = \infty$. Indeed, if $z_1 = \infty$ we may take $g_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and if $z_1 \neq \infty$ we may take $g_1 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & z_1 \end{smallmatrix}\right)$.

Next we claim that there exists $g_2 \in GL(2,F)$ such that $g_2 \cdot \infty = \infty$ and $g_2 g_1 \cdot z_2 = 0$. Indeed, since $z_1 \neq z_2$, $g_1 \cdot z_2 \neq g_1 \cdot z_1 = \infty$ and so we may take

$$g_2 = \begin{pmatrix} 1 & -g_1 z_2 \\ 0 & 1 \end{pmatrix}.$$

Next we claim that there exists $g_3 \in GL(2,F)$ such that $g_3 \cdot \infty = \infty$, $g_3 \cdot 0 = 0$ and $g_3 g_2 g_1 \cdot z_3 = 1$. Indeed, we have $g_2 g_1 \cdot z_1 = \infty$ and $g_2 g_1 \cdot z_2 = 0$. Since z_1, z_2 and z_3 are all distinct, $g_2 g_1 \cdot z_3 \neq 0, \infty$. We may then take

$$g_3 = \begin{pmatrix} 1 & 0 \\ 0 & g_2 g_1 \cdot z_3 \end{pmatrix}.$$

Now letting $g = g_3 g_2 g_1$ we have $g \cdot z_1 = \infty$, $g \cdot z_2 = 0$ and $g \cdot z_3 = 1$. ∎

If a group G acts on a set X, a *fixed point* of $g \in G$ is an element $x \in X$ such that $g \cdot x = x$.

Proposition 32. *If $g \in GL(2,F)$ has three fixed points then g is a scalar matrix and g acts trivially.*

Proof. Let z_1, z_2 and z_3 be distinct fixed points of g. Let $h \in GL(2,F)$ satisfy $h(z_1) = \infty$, $h(z_2) = 0$ and $h(z_3) = 1$. Then hgh^{-1} fixes ∞, 0 and 1, for example $hgh^{-1} \cdot \infty = hg \cdot z_1 = h \cdot z_1 = \infty$.

Let $hgh^{-1} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Since

$$\infty = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}$$

we have $c = 0$. Now since

$$0 = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} 0 = \frac{b}{d}$$

we have $b = 0$. Finally, since

$$1 = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} 1 = \frac{a}{d}$$

we have $a = d$. Thus $hgh^{-1} = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ is a scalar matrix. Now $g = h^{-1}\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)h$ and since the scalar matrices are in the center of $GL(2,F)$ we have $g = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$, as required. ∎

We now prove Theorem 29. We take $F = \mathbb{Z}_5$ to be the field with five elements. Thus $GL(2,F)$ acts on the set $\mathbb{P}^1(F) = \{0, 1, 2, 3, 4, \infty\}$ with six elements. We label the six corners of the cube which are moved by R and U by these six elements as in Figure 37.

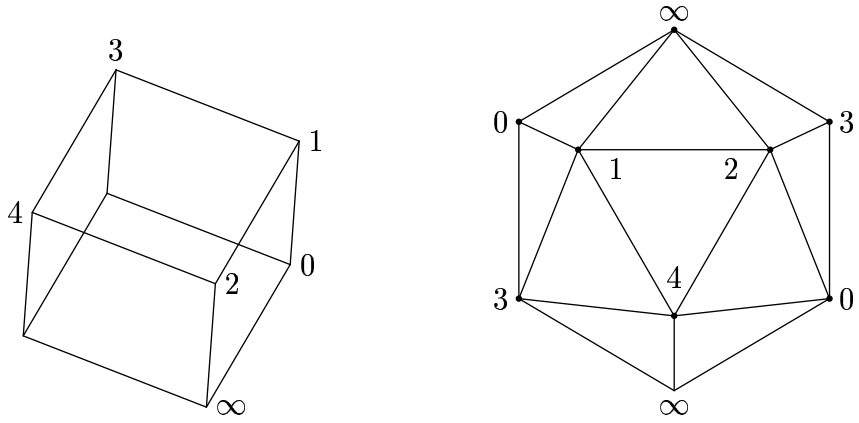

Figure 37. Labelling the corners and the icosahedron by $\mathbb{P}^1(\mathbb{Z}_5)$.

Proposition 33. *With the six vertices labelled as in Figure 37, every operation of the group $\mathfrak{T}$ is given by a linear fractional transformation.*

Proof. Since a composition of linear fractional transformations is a linear fractional transformation, it is sufficient to check this for the generators R and U. First R is the 4-cycle $(10\infty 2)$, and one checks directly that this coincides with the linear fractional tranformation represented by the matrix $\left(\begin{smallmatrix}1&4\\3&0\end{smallmatrix}\right)$. On the other hand the operation U IS the 4-cycle (1243), which coincides with the linear fractional transformation represented by the matrix $\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)$. The theorem follows. ■

Now Theorem 29 follows from Proposition 32, since if a linear fractional fixes three points it must fix everything.